

 ~ 201

 ~ 202

inter to the state

111 112 1111

IDENTIFICATION CERTIFICATE (IDC) CERTIFICATE AUTHORITY (CA) IDENTIFICATION AUTHORITY (IDA) PUBLIC KEY CERTIFICATE (PKC) Ę 204 SERVICE PROVIDER (SP) (CONTENT DISTRIBUTION) SERVICE PROVIDER (SP) (SETTLEMENT AGENCY) FIG. 2 ENCRYPTED DATA COMMUNICATION IDENTIFICATION OF USER B IDENTIFICATION OF USER A ENCRYPTED DATA COMMUNICATION 203 USER DEVICE A (USER A) USER DEVICE B (USER B) ENCRYPTED DATA COMMUNICATION 206 205 IDENTIFICATION OF USERS A AND B

ltem	Description	Value employed in the present IA
	Version 1	
version	Version of the certificate format	V3
serial Number	Serial number of the certificate assigned by the IA	Assigned in a serial fashion
signature algorithm Identifier algorithm parameters	Algorithm of the signa- ture of the certificate and parameters thereof	Elliptic curve number/RSA parameters when an elliptic curve is used Key length when RSA is employed
issuer	IA name (in a distiguished name form)	Name of the present IA
validity notBefore notAfter	Period during which the certificate is valid Start date Expiration date	
subject	Name which identifies the user	User device ID or ID of the service subject
subject Public Key Info algorithm subject Public key	Information of the public key of the user Algorithem of the key Key	Elliptic curve/RSA Public key of the user
	Version 3	
authority Key Identifier key Identifier authority Cert Issuer authority Cert Serial Number	tion of the IA Key identification number (octal number)	
subject key Identifier	Used when a plurality of keys are certified	Not used
key usage (0)digital Signature (1)non Repudiation (2)key Encipherment (3)data Encipherment (4)key Agreement (5)key CertSign (6)cRL Sign	Specifying the purpose of the key (0)for digital signature (1)to prevent repudiation (2)for encryption of the Key (3)for encryption of a message (4)for use in transmission of a symmetric key (5)used to verify the certificate (6)used to verify the signature of the certificate revolution list	0,1,4, or 6 is used
private Key Usage Period notBefore notAfter	Period during which the private key stored in the user is valid	Usage period is the same for the certificate, the public key, and the private Key (default)

Certificate Policy policy Identifier policy Qualifers	Certificate policy of the certificate authority Policy ID (according to ISO/IEC9834-1) Certification criteria		
policy Mappings issuer Domain Policy subject Domain Policy	Required only when the CA is certificated. Mappings of the policy of the issuer domain policy and the subject domain policy are defined	default = none	
supported Algorithms algorithm Identifier intended Usage intended Certificate Policies	Attributes of the directory (X.500) are defined. Used to inform a receiving party of communication of the attributes the direction so that the receiving party can use the direction information	default = none	
subject Alt Name	Alternative name of the user (in the form of GN)	not used	
issuer Alt Name	Not used although this item is included in the certificate format (default = none)	default = none	
subject Directory Attributes	Arbitrary attributes of the user	not used	
basic Constraints	Specifies the public key to be certified		
cA path Len Constraint	Indicates whether the public key is used by a user or by a certificate authority to write a signature	default = used by a user	
name Constraints permitted Subtrees base minimum	Used only when the certification is to certify a certification authority (CA)	default = none	
maximum excluded Subtrees			
policy Constraints requier Explicit Policy inhibit Policy Mapping	Constraints are described in terms of requirements of explicit policy ID or inhibit policy mapping for the remaining certification path		
CRL Distribution Points	Indicates a reference point in the revocation list at which data is present which indicates whether the certificate of a user is revocated	Pointer which points to a location where the certificate is registered. The revocation list is managed by an issuer	
Signature	Signature of the issuer		

	Version	Version
	Serial Number	Identification Number
Indis-	signature algorithm	Signature algorithem
	algorithm parameters	Algorithm Parameters
pensable Items	Issuer	Name of the identification authority (in the form of a distinguished name)
· · · · · · -	Validity notBefore notAfter	Period during which the certificate is valid Start date Expiration date
	Subject	Name of the subject to be certificated (in a DN form)
	subject Template Info encrypt Type encrypt Unique ID encryption Algorithm parameter	Template information
	validity subject Template Source subject Template	 Validity period (start date, expiration date) Type of the template Template
	Subject PKC info subject PKC serial Number	Information about the public key certificate of the subject
Extended Items		public key certificate Unique ID of the issuer
	Issuer Unique ID	Unique ID of the subject
	Subject Unique ID Public Key Certificate	Public key certificate
	Issuer Alt Name	Alternative name of the issuer
	subject Directory Attributes	Personal information (encrypted as required) information used to authenticate subject Age, sex, etc.
	Valid Count	Number of times the certificate is allowed to be used
	Control Table Link Info Ctl Tbl Location Ctl Tbl Unique ID	Link information describing group information • Location of a link information control table (URL, IP address, etc.) • Identification number of the link information
Indispen- sable	IDA Signature	Signature of the IDA

FIG. 6A

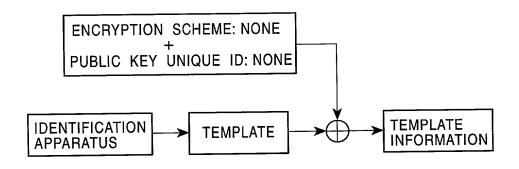


FIG. 6B

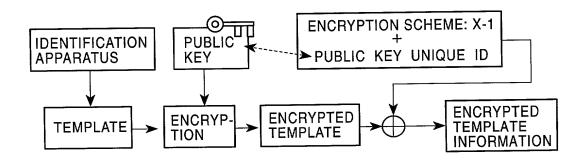
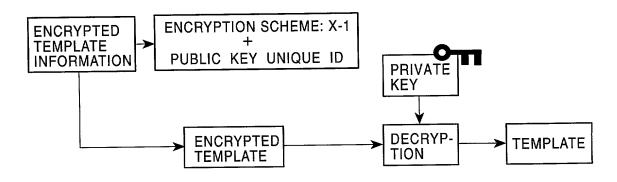


FIG. 6C



THE PARTY OF THE P

PUBLIC KEY USED TO ENCRYPT TEMPLATES	EXAMPLES OF MANNERS IN WHICH TEMPLATE INFORMATION STORAGE IDC IS USED
PUBLEC KEY OF A USER OR A USER DEVICE	TO IDENTIFY AN AUTHORIZED USER OF A USER DEVICE (SUCH AS A PC) ON THE BASIS OF AN IDENTIFICATION CERTIFICATE OF THE USER
PUBLIC KEY OF A SERVICE PROVIDER	USED BY A SERVICE PROVIDER TO IDENTIFY A PARTICULAR USER SUCH AS A USER TO WHOM SERVICE IS TO BE PROVIDED, ON THE BASIS OF AN IDENTIFICATION CERTIFICATE (IDC) OF THE USER
PUBLIC KEY OF AN IDENTIFICATION AUTHORITY	IN DATA TRANSMISSION AMONG VARIOUS TERMINALS, A SENDER OR A RECEIVER IDENTIFIES

FIG. 8A

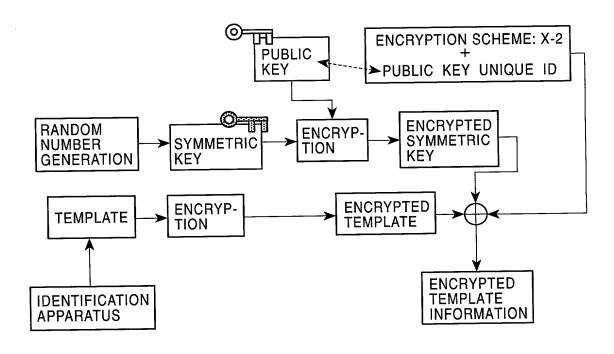


FIG. 8B

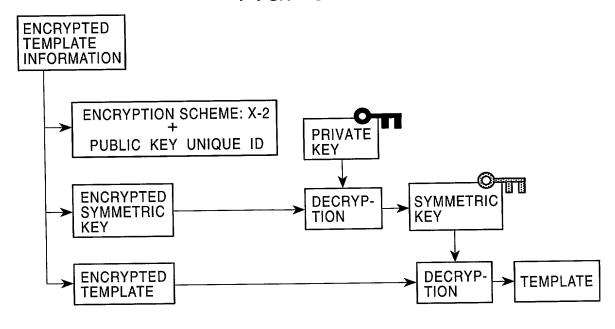
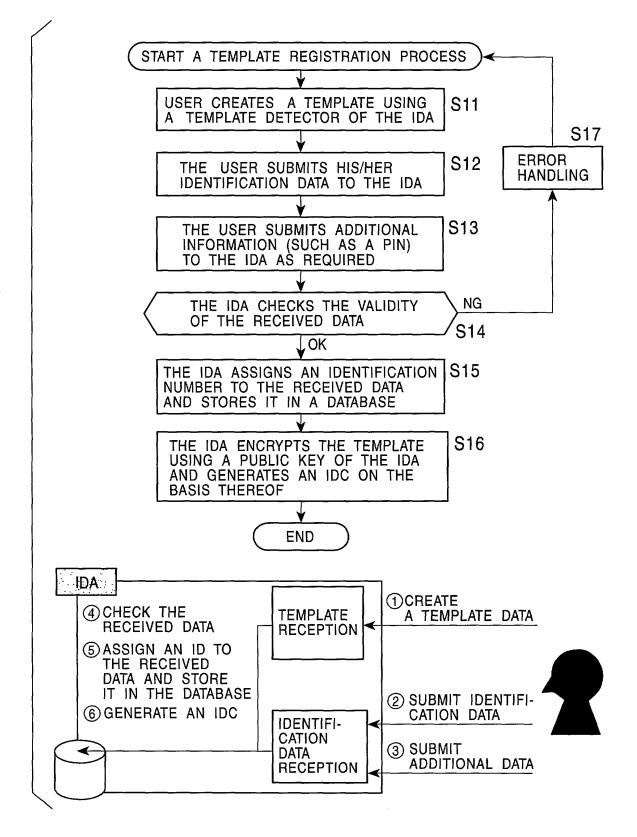


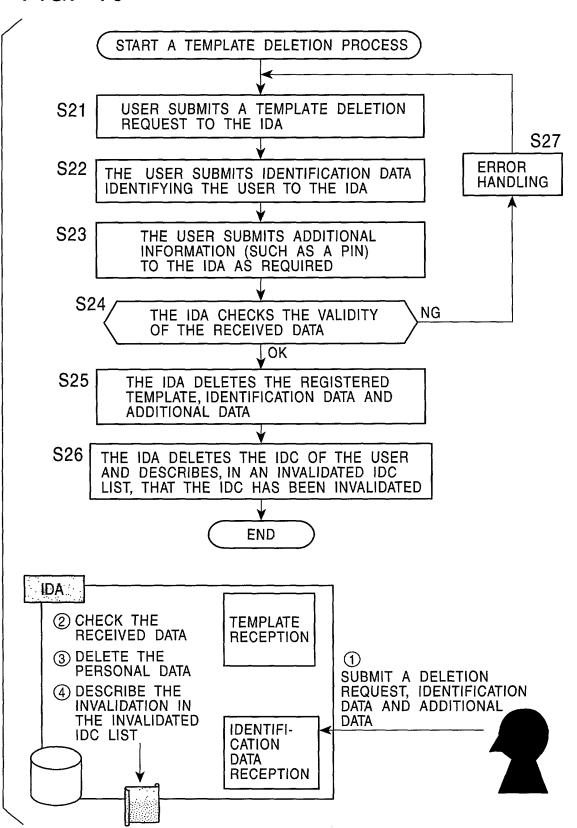
FIG. 9

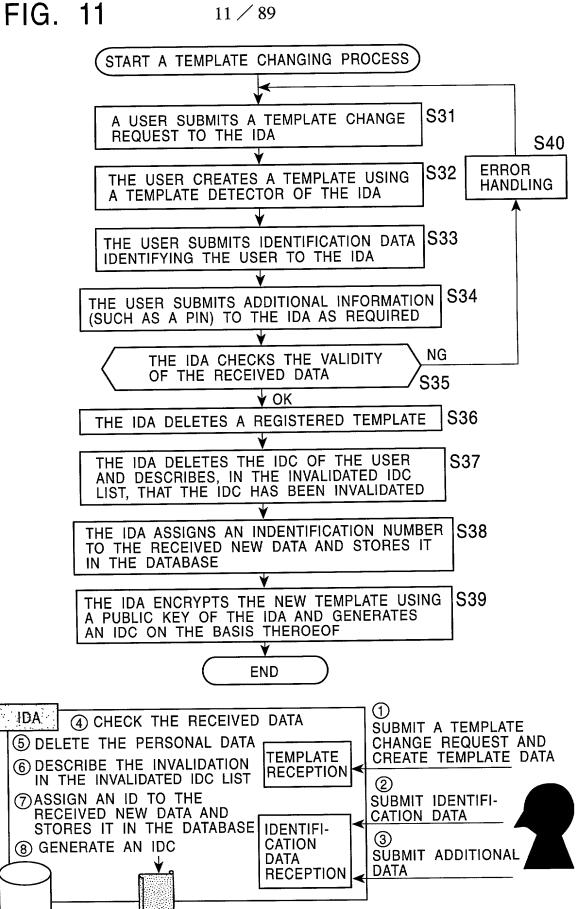


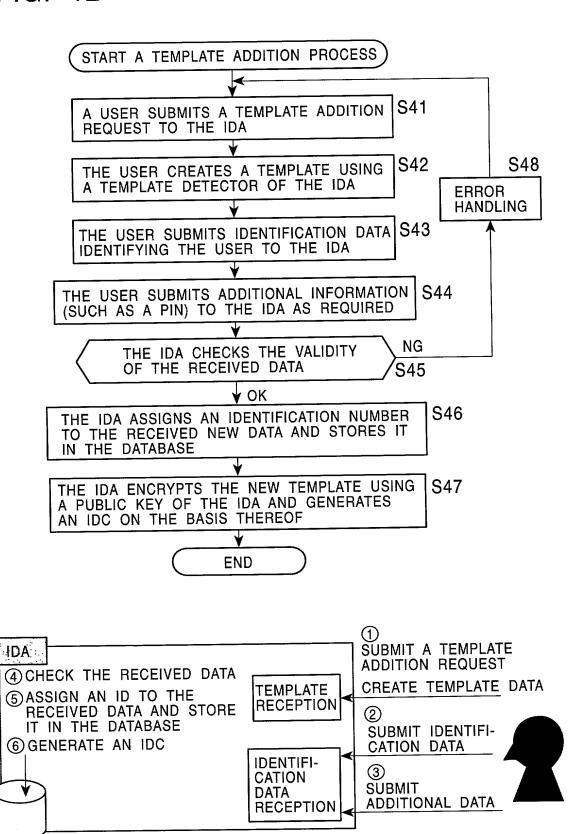
i.

pp in the

FIG. 10







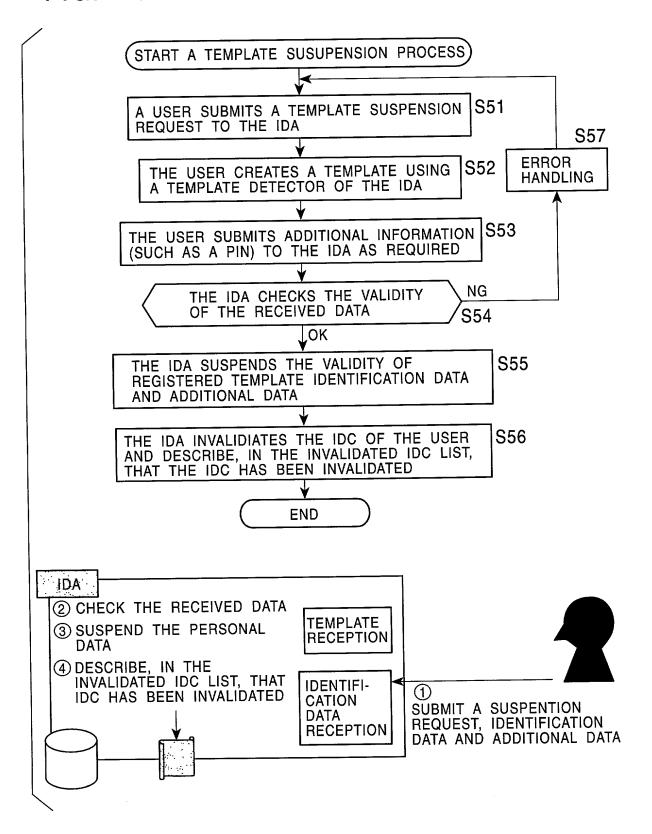
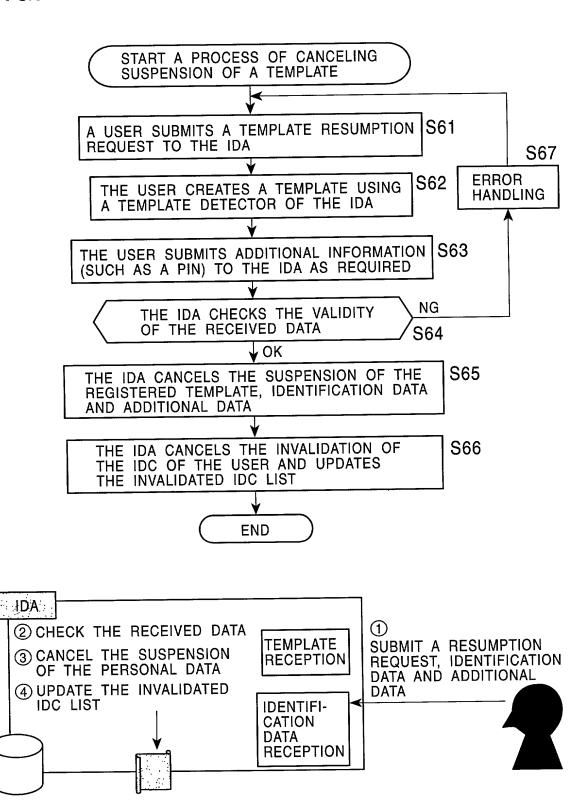
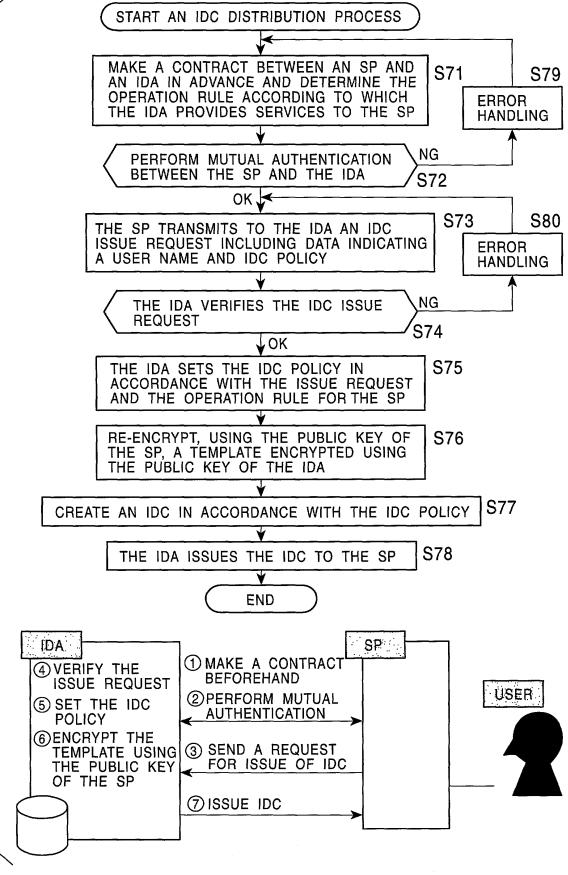


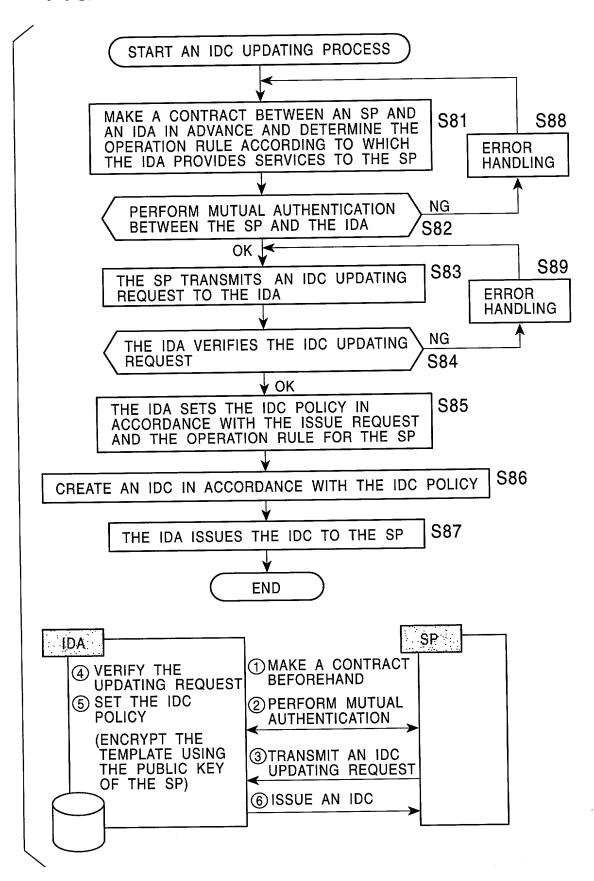
FIG. 14





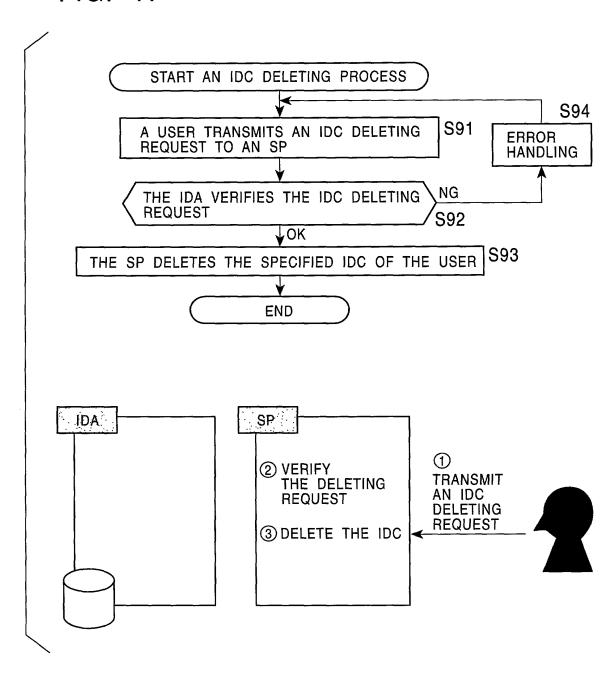
2411 HE HE HE

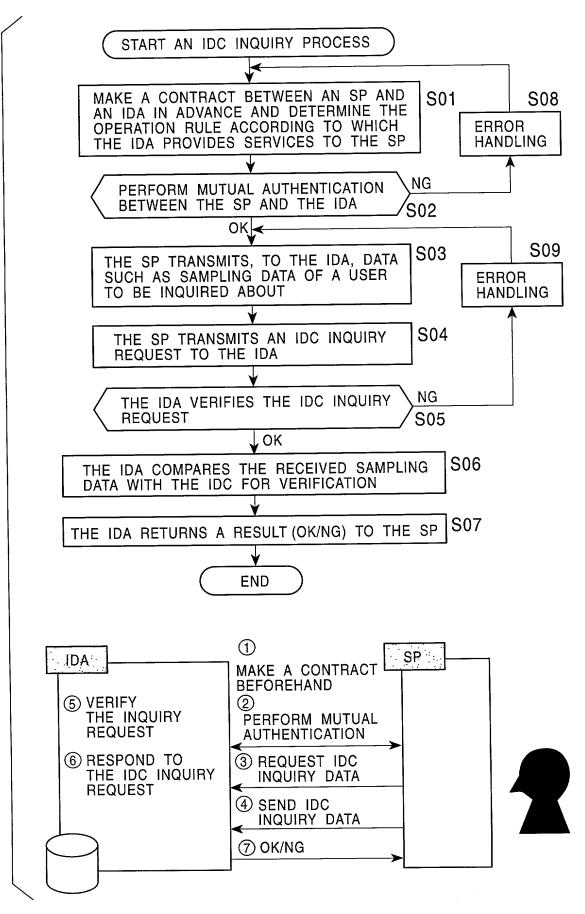
FIG. 16

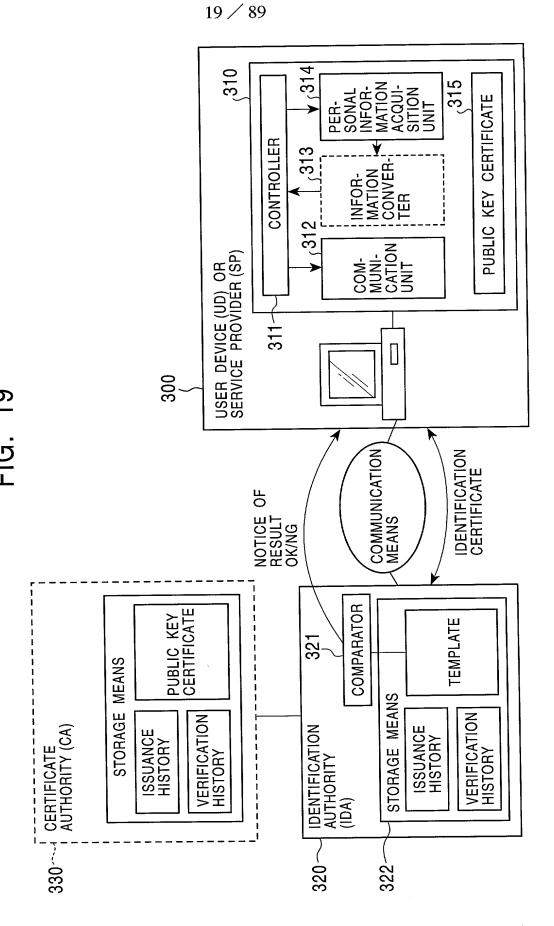


11 1 DB0.03938311 (

FIG. 17







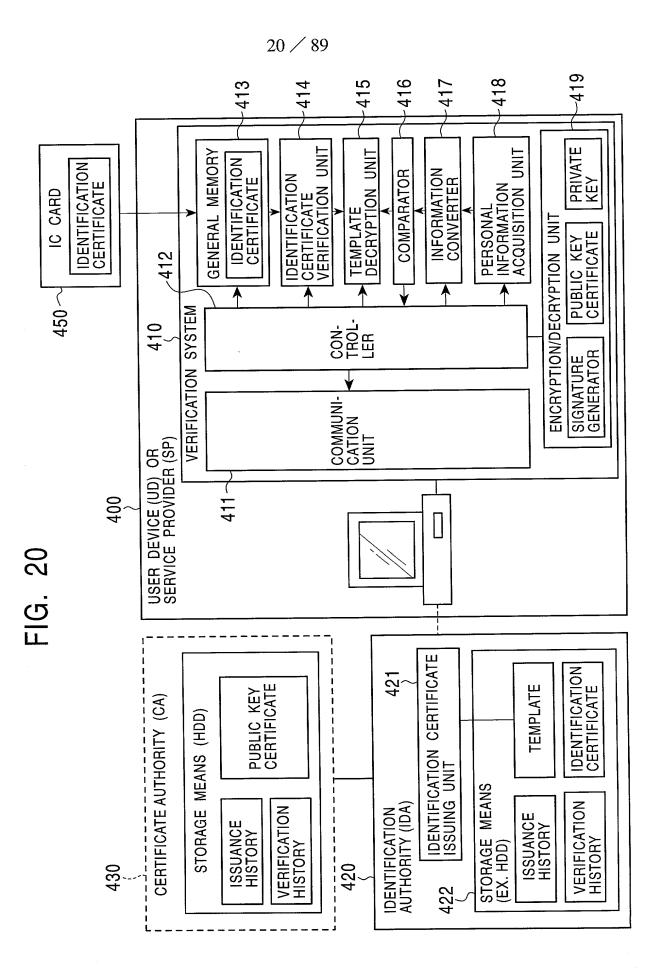


FIG. 21A

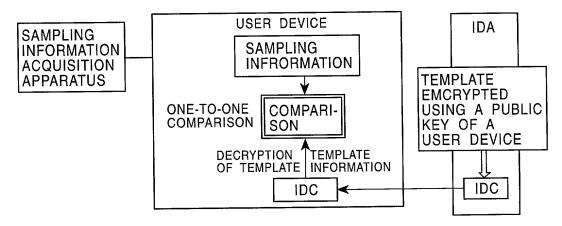


FIG. 21B

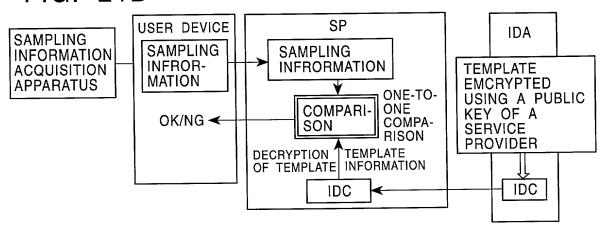


FIG. 21C

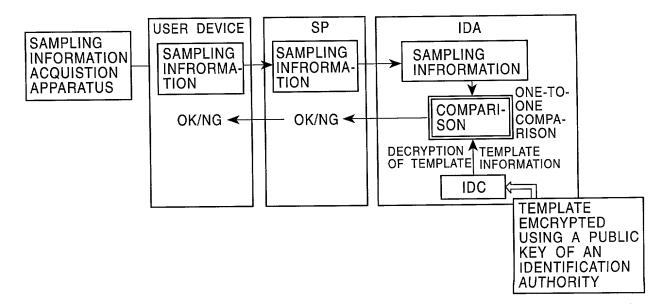
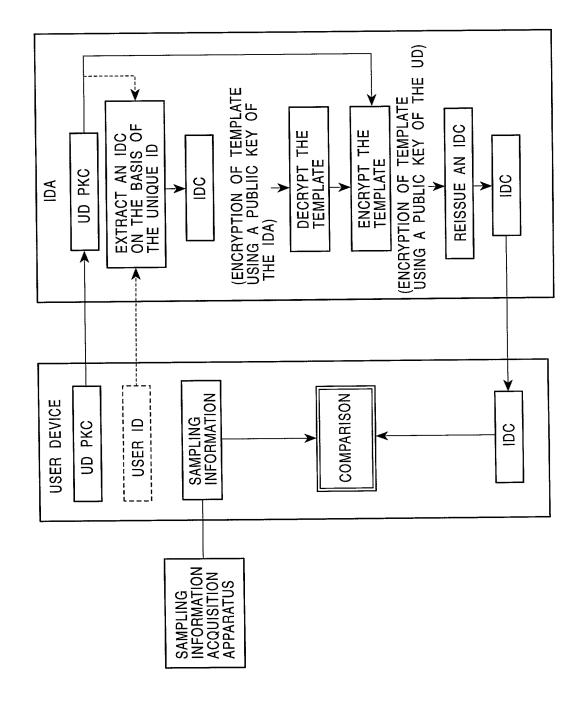


FIG. 22



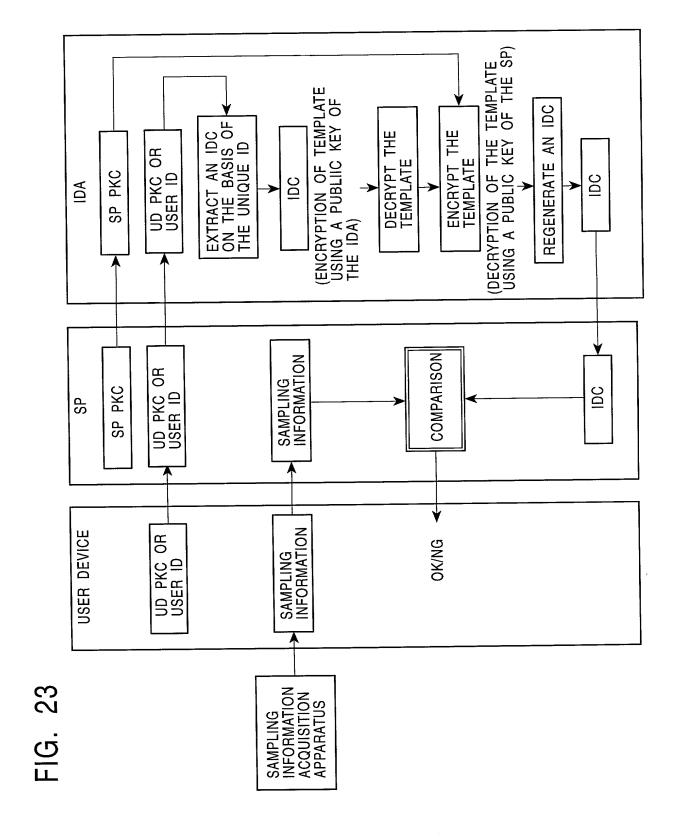


FIG. 24

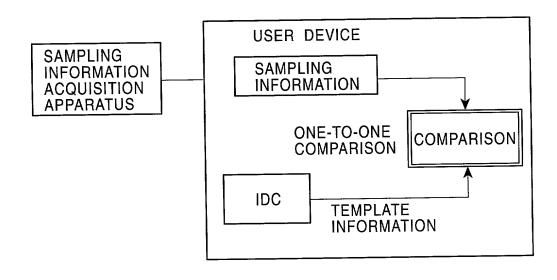


FIG. 25

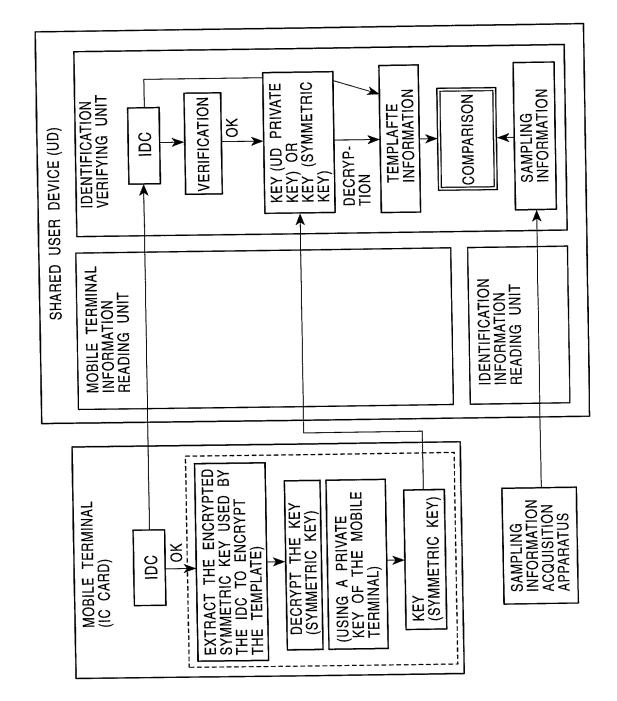


FIG. 26

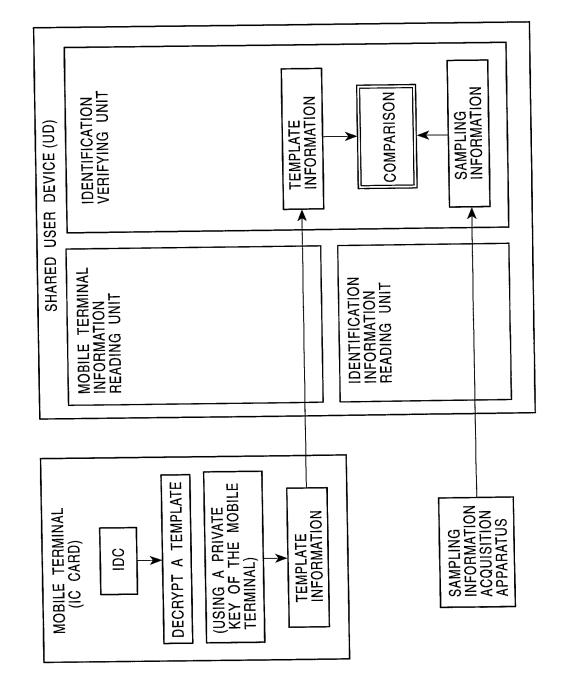


FIG. 27

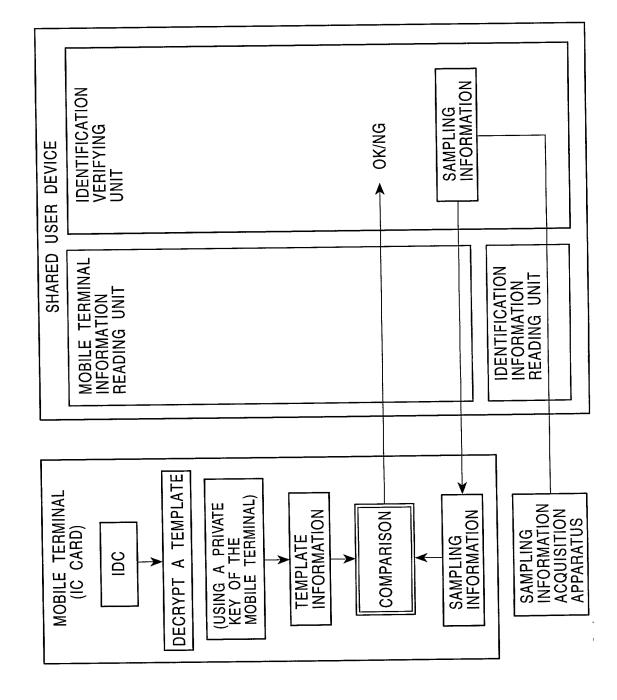
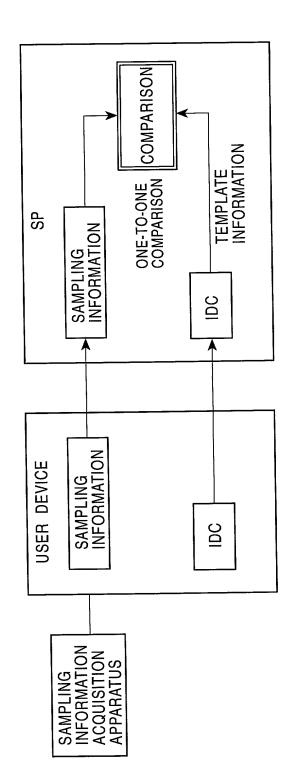
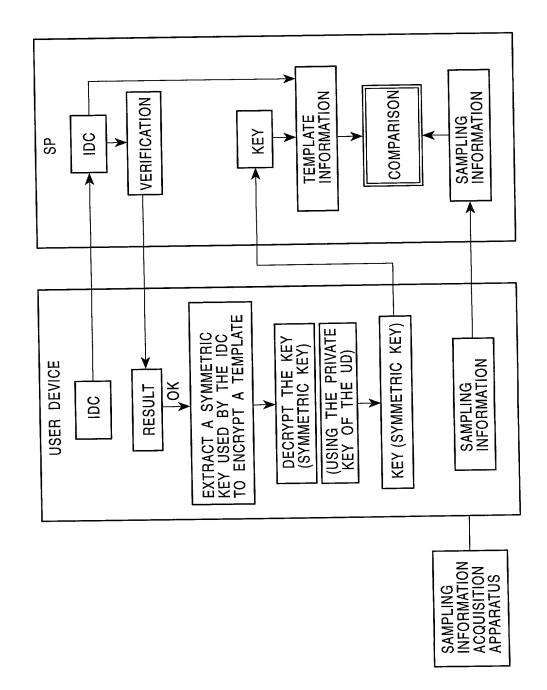


FIG. 28



a paint is nicht time (fiel)

FIG. 29



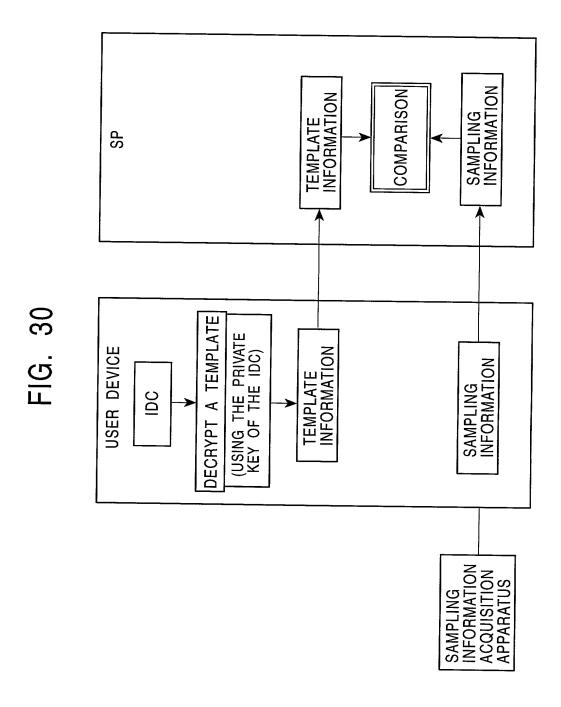


FIG. 31

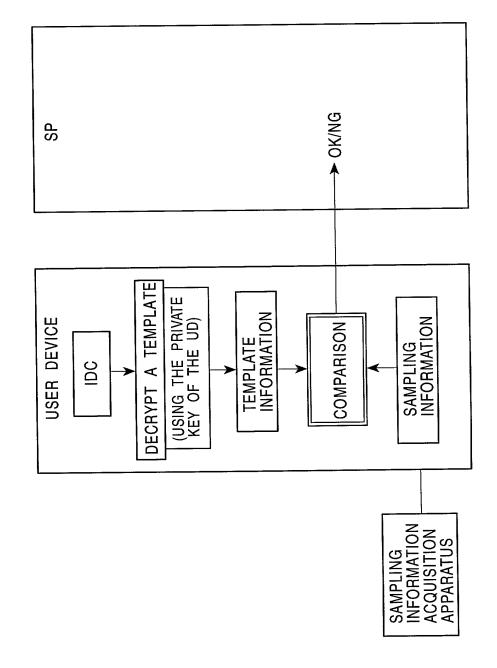


FIG. 32

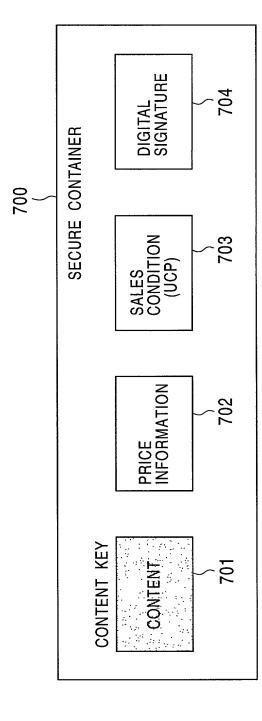


FIG. 33

and the same of th	The state of the s
USER ID	IDENTIFICATION CERTIFICATE (IDC) IDENTIFIER
ABC0001	CDE00021
ABC0002	CDE00027
ABC0003	CDE03211
:	•
BBC0231	EED02333

	DATA TYPE	
	TYPE OF DEALING POLICY	
PERIOD D	URING WHICH DEALING POLICY IS VALID	
	CONTENT ID	
	CONTENT PROVIDER ID	
	DEALING POLICY ID	I
VE	RSION OF THE DEALING POLICY	
	AREA CODE	
	USABLE DEVICE CONDITIONS	
USER	S PERMITTED TO USE THE CONTENT	
	IDC IDENTIFIER LIST	~711
	SERVICE PROVIDER ID	
UCP G	ENERATION MANAGEMENT INFORMATION	~712
MAXIMUI DISTRIBI	M ALLOWABLE NUMBER OF SECONDARY JTIONS	~713
	NUMBER OF RULES	
	RULE ADDRESS	
	RULE NUMBER	
RULE 1	TYPE OF PERMITTED USAGE	
:	: :	
	RULE NUMBER	1
RULE N	TYPE OF PERMITTED USAGE	
(INDIC	CATION OF WHETHER THE SIGNATURE BEEN VERIFIED)	
	PUBLIC KEY CERTIFICATE	
	SIGNATURE	

FIG. 35

RULE NUMBER	PERMITTED USAGE	PERIOD	NUMBER OF TIMES CONTENT IS USED	COPY	
1		NOT LIMITED	NOT LIMITED	_	
2	PLAYBACK	LIMITED	NOT LIMITED	_	
3		NOT LIMITED	LIMITED	_	
4		NOT LIMITED	NOT LIMITED	NOT LIMITED	
5		LIMITED	NOT LIMITED	NOT LIMITED	
6		NOT LIMITED	LIMITED	NOT LIMITED	
7		NOT LIMITED	NOT LIMITED		
8	COPY	LIMITED	NOT LIMITED	SCMS	
9		NOT LIMITED	LIMITED		
10		NOT LIMITED	NOT LIMITED		
11		LIMITED	NOT LIMITED	OTHERS	
12		NOT LIMITED	LIMITED		
13	CHANGING OF PERMITTED USAGE				
14	REDISTE	RIBUTION			
15	UPGRADE TO AN ALBUM				
16	PERMISSION OF TRANSFERRING MANAGEMENT				

	DATA TYPE	
	TYPE OF PRICE INFORMATION	l
PERIOD I	DURING WHICH THE PRICE INFORMATION	
	CONTENT ID	
	SERVICE PROVIDER ID	
	PRICE INFORMATION ID	
VE	RSION OF THE PRICE INFORMATION	
	AREA CODE	
	USABLE DEVICE CONDITIONS	
USER	S PERMITTED TO USE THE CONTENT	
	IDC IDENTIFIER LIST	
	CONTENT PROVIDER ID	
	DEALING POLICY ID	
	NUMBER OF RULES	
	RULE ADDRESS	
	RULE NUMBER	
RULE 1	<u>:</u>	
÷	<u>:</u>	
	RULE NUMBER	
RULE N	:	
(INDIC HAS	CATION OF WHETHER THE SIGNATURE BEEN VERIFIED)	
	PUBLIC KEY CERTIFICATE	
	SIGNATURE	}

FIG. 37

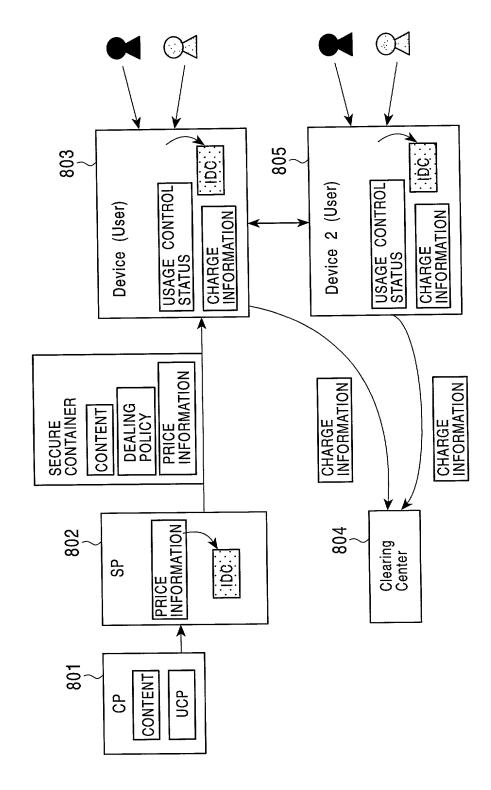
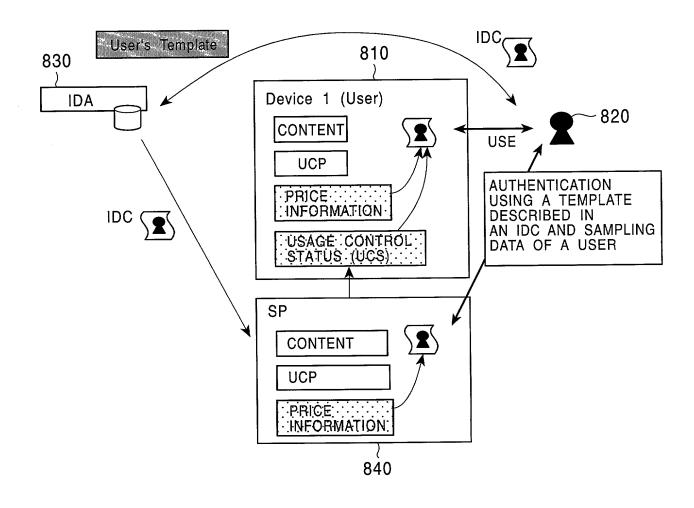
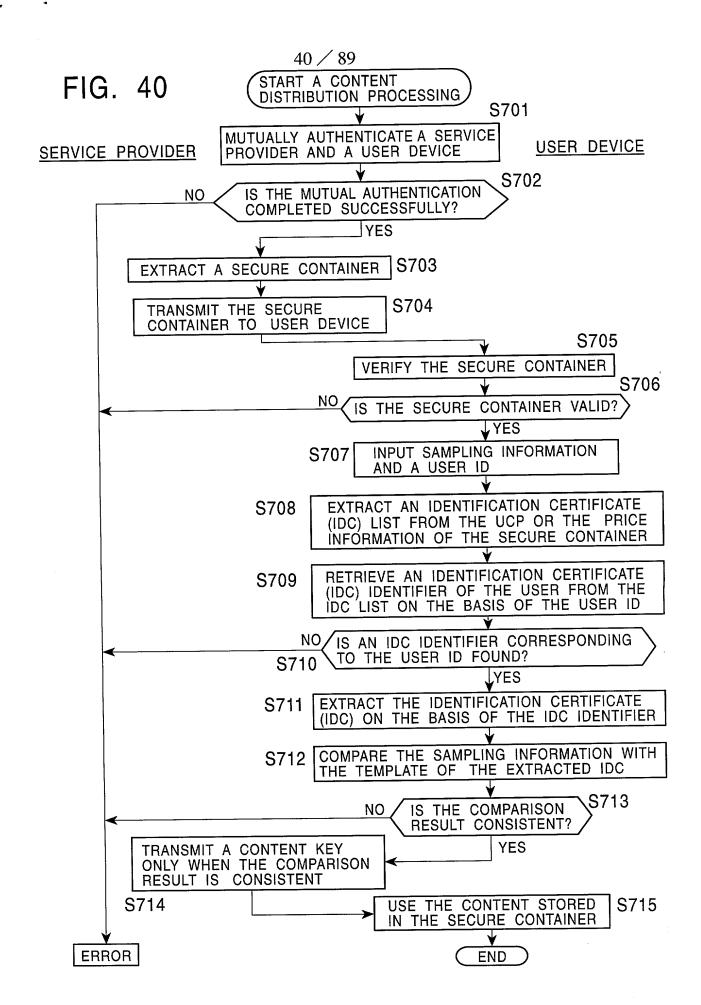


FIG. 38

DATA TYPE	
TYPE OF USAGE PERMISSION CONDITION INFORMATION	
PERIOD DURING WHICH THE USAGE PERMISSION CONDITION INFORMATION IS VALID	
CONTENT ID	
ALBUM ID	
ENCRYPTION PROCESSING UNIT ID	
USER ID	
CONTENT PROVIDER ID	
DEALINGF POLICY ID	
VERSION OF DEALING POLICY	
SERVICE PROVIDER ID	<u> </u>
PRICE INFORMATION ID	
VERSION OF PRICE INFORMATION	
ID OF USAGE PERMISSION CONDITION INFORMATION	
RULE NUMBER OF PERMISSION FOR PLAYBACK (USAGE)	
PERMITTED USAGE NUMBER	
NUMBER OF TIMES THE CONTENT IS ALLOWED TO BE FURTHER PLAYED BACK	
PERIOD DURING WICH THE PLAYBACK PERMISSION IS VALID	
RULE NUMBER OF PERMISSION FOR COPYING (USE)	
USAGE PERMISSION NUMBER	
NUMBER OF TIMES THE CONTENT IS ALLOWED TO BE FURTHER COPIED	
UCS GENERATION MANAGEMENT INFORMATION	732
NUMBER OF TIMES UCS IS ALLOWED TO BE SECONDARILY DISTRIBUTED	733
IDC IDENTIFIER LIST	731
ID OF THE ENCRYPTION PROCESSING UNIT HAVING PERMISSION IN TERMS OF PLAYBACK	

FIG. 39





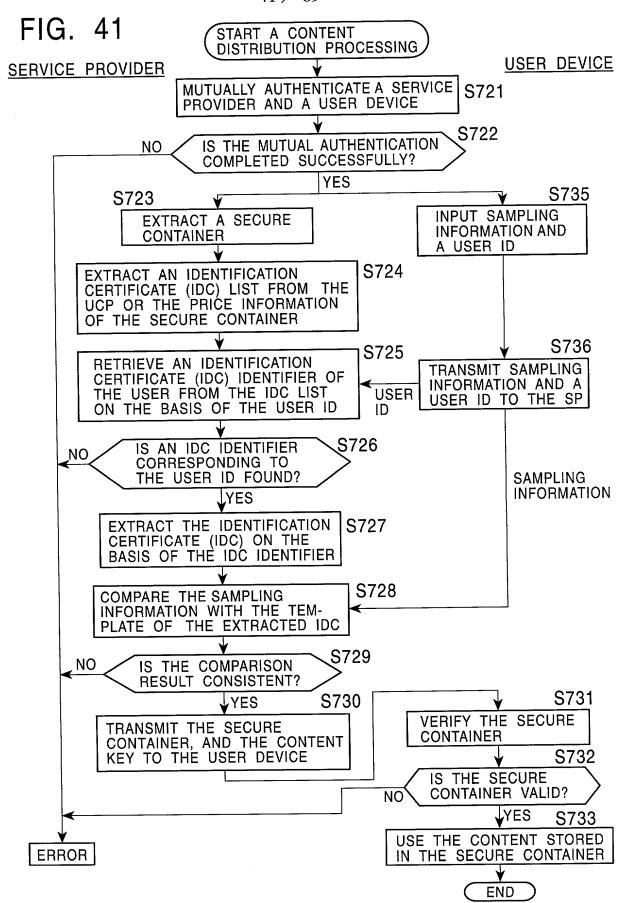
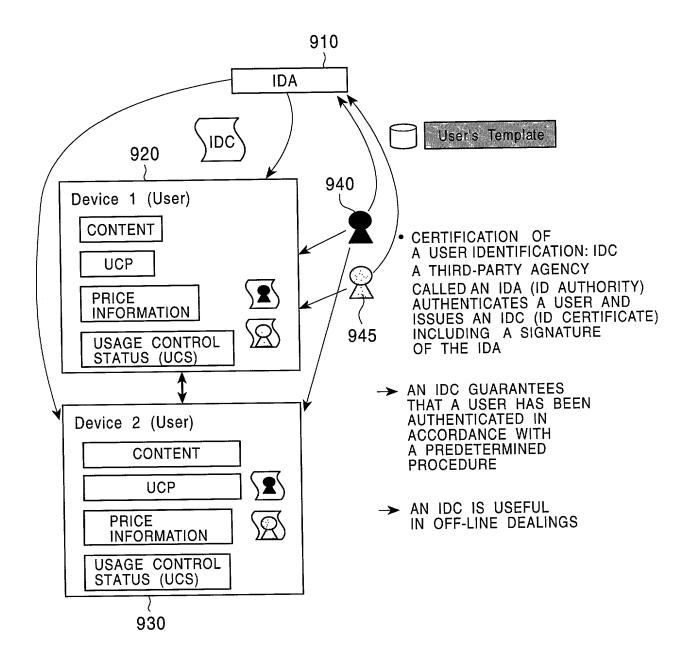
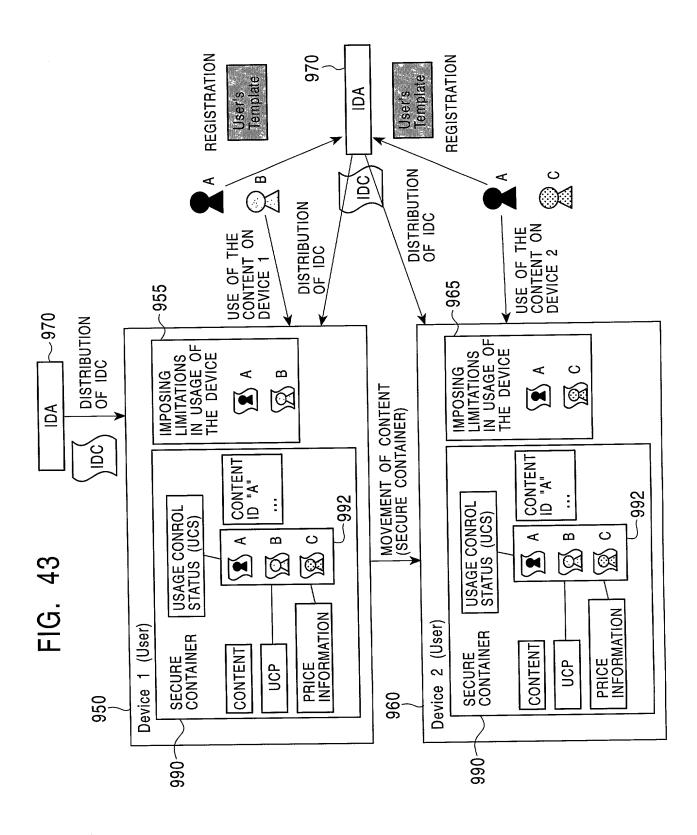
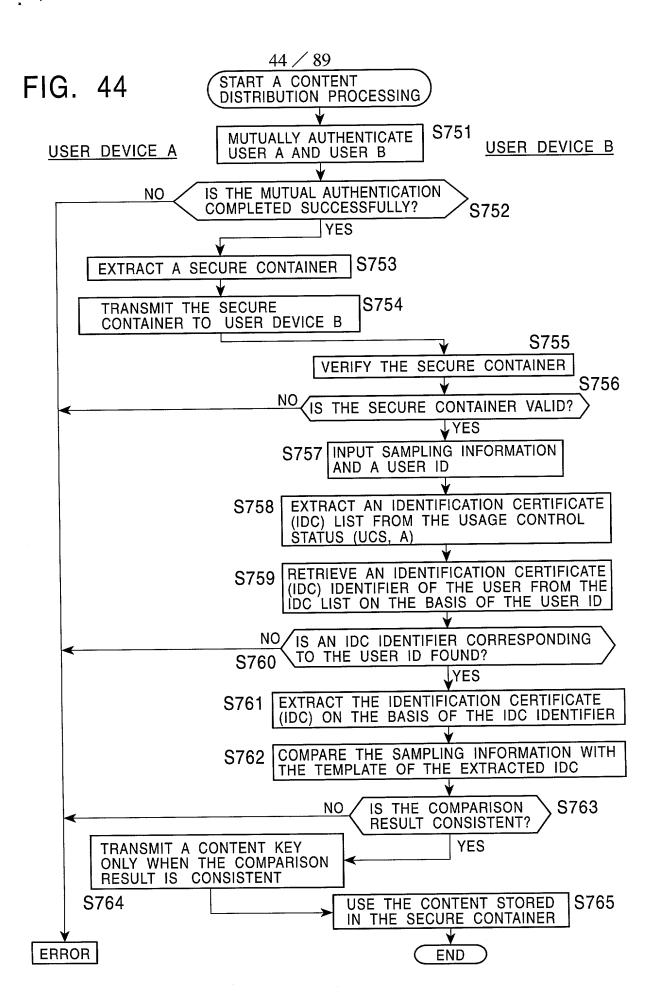
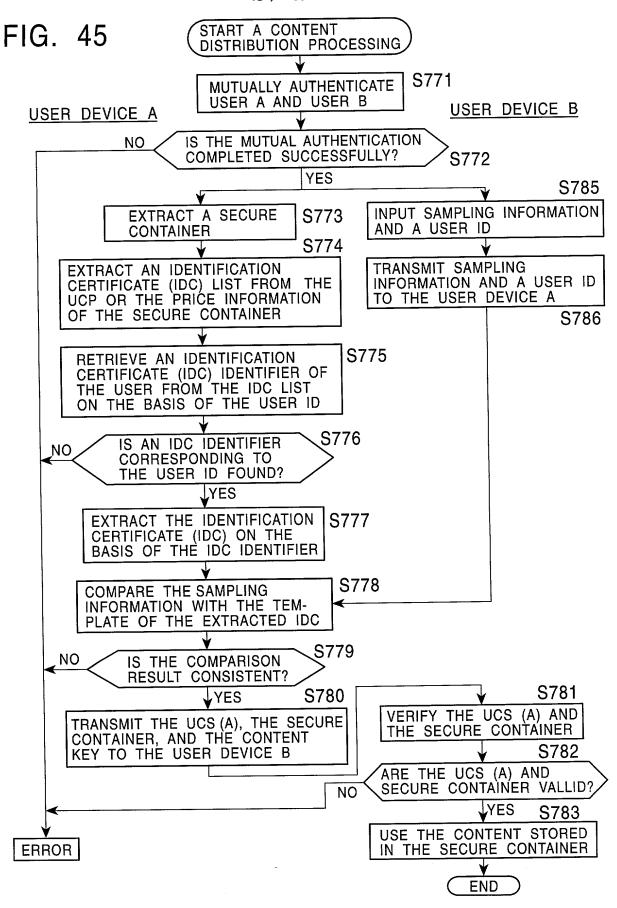


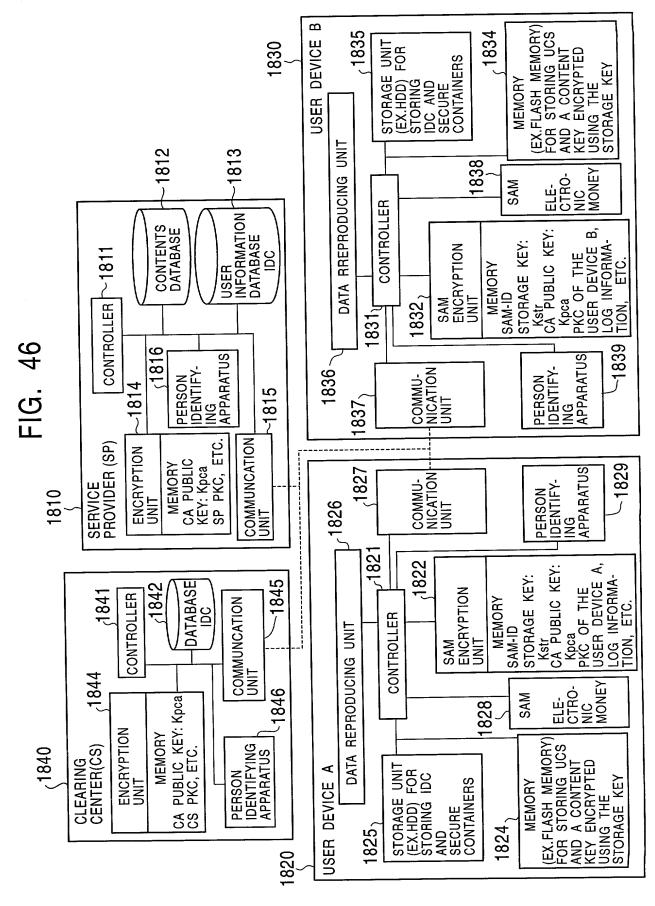
FIG. 42











DISTERBE CESCIA

FIG. 47A

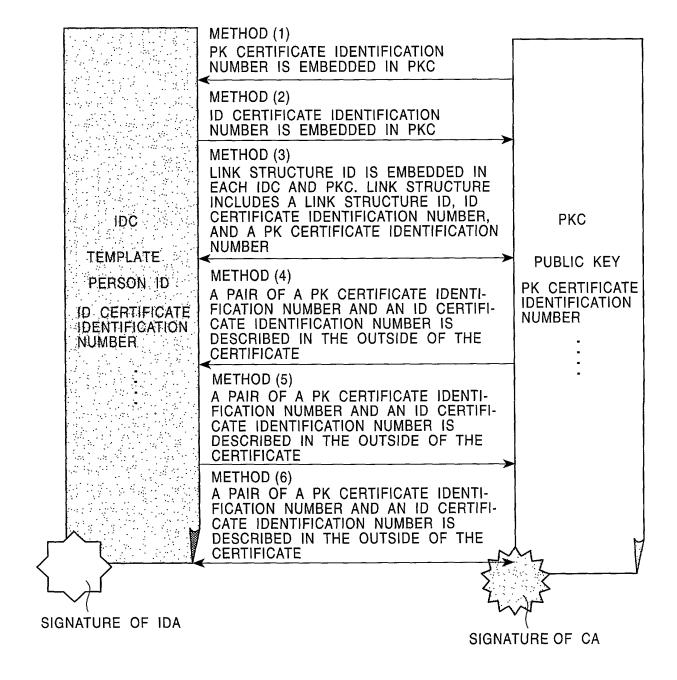


FIG. 47B

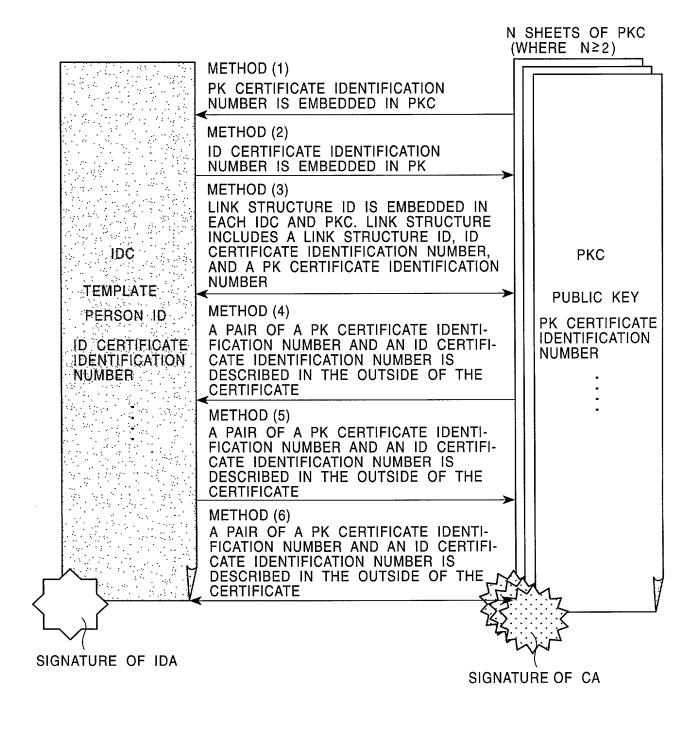


FIG. 48A

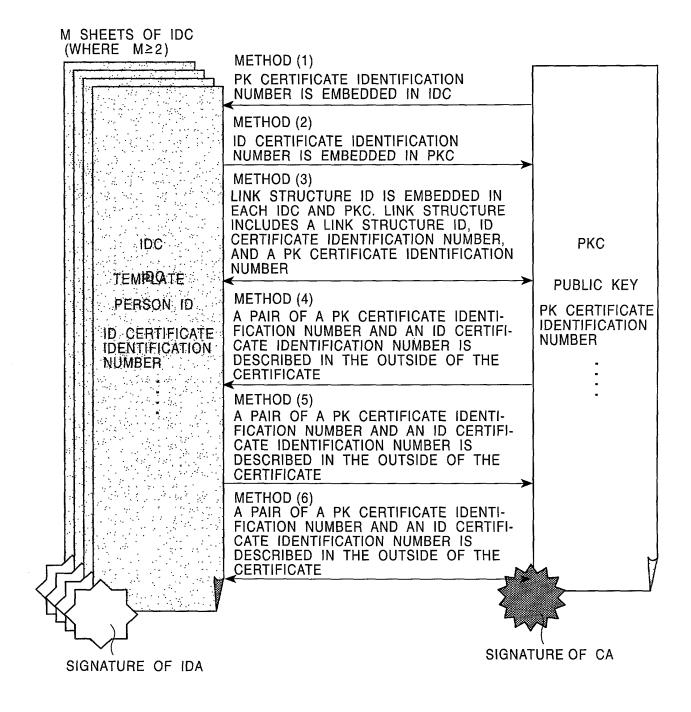


FIG. 48B

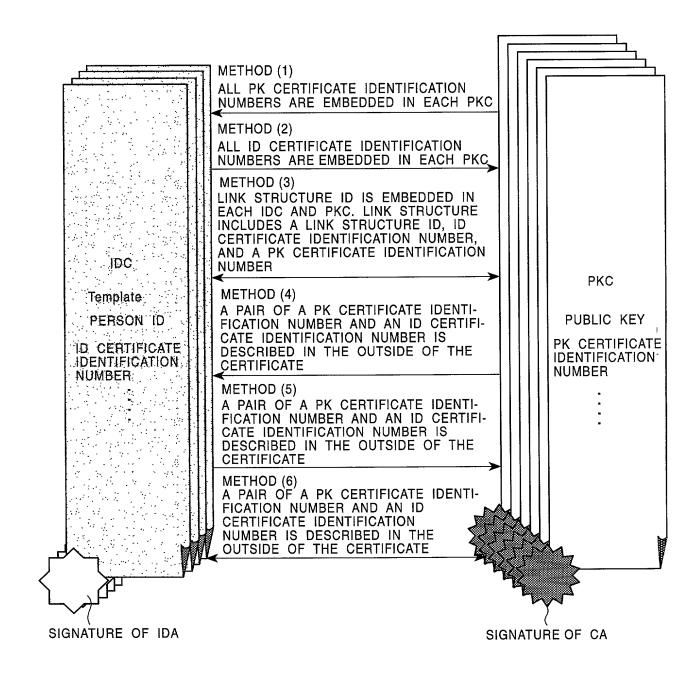


FIG. 49A

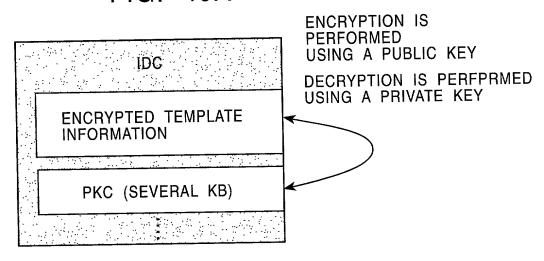
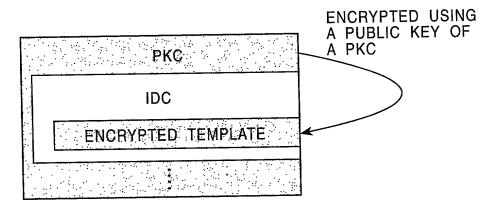
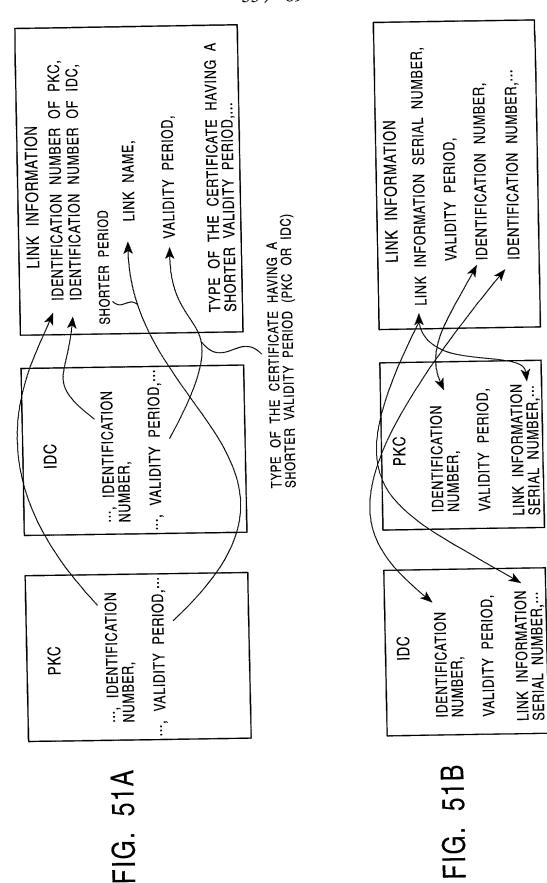


FIG. 49B



PUBLIC: KEY PUBLIC KEY IDENTIFICATION NUMBER,... PKC PKC ..., ENCRYPTE CERTIFICATE OF A PUBLIC KEY USED IN THE SERVICE | IDENTIFICATION | NUMBER OF THE | PUBLIC KEY USED | IN ENCRYPTION ENCRYPTION ENCRYPTED TEMPLATE ENCRYPTED TEMPLATE IDENTIFICATION NUMBER: IDENTIFICATION NUMBER. FIG. 50B ç. Ç.

FIG. 50A



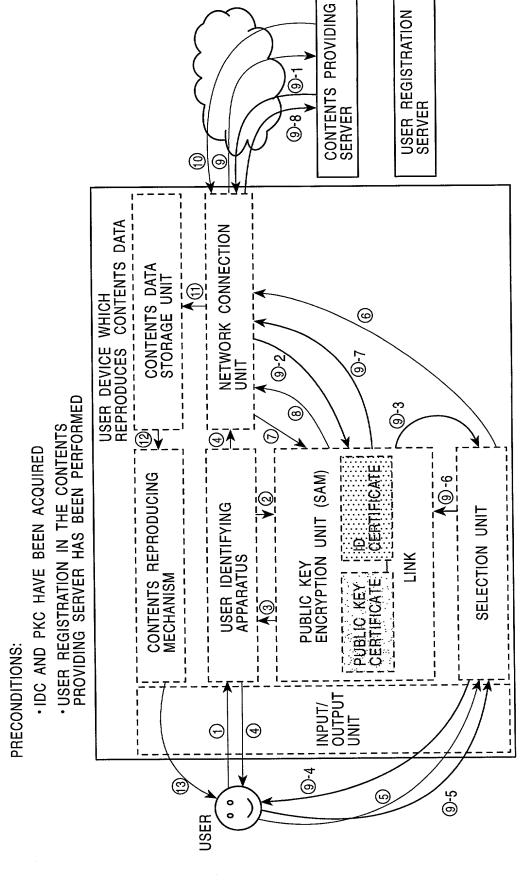
na Turnel attribute (d. 1. 1937).

10.1 1408-18038 [1]

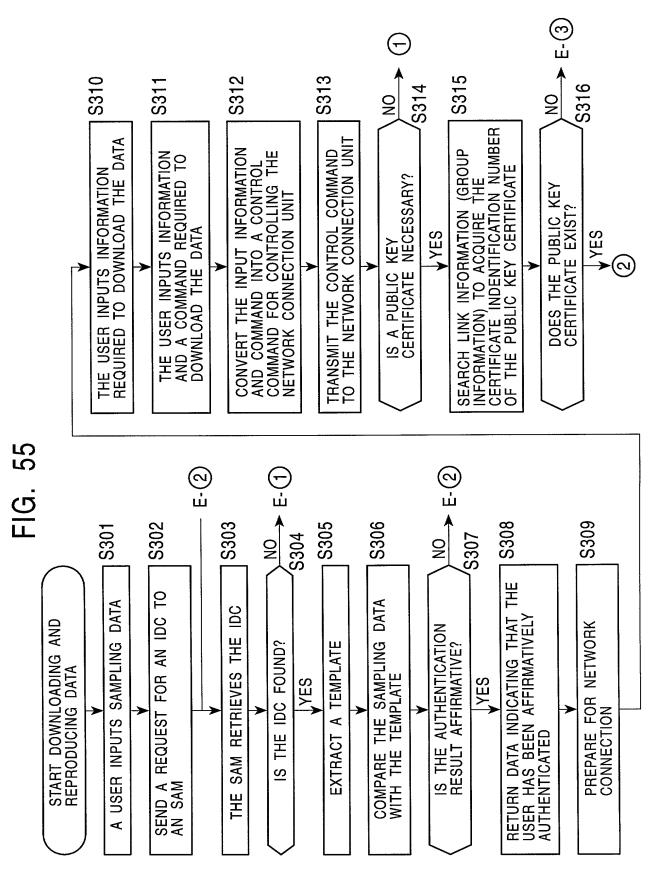
CONTENTS/ PROVIDING SERVER USER REGISTRATION SERVER NETWORK (EX. THE INTERNET) 502 NETWORK CONNECTION UNIT 504 CONTENT DATA STORAGE UNIT 500 USER DEVICE WHICH PLAYS BACK CONTENT DATA -503 ~ 506 ~502 FIG. 53 CONTENTS REPRODUCING MECHANISM PUBLIC KEY ENCRYOTION UNIT (SAM) USER IDENTIFYING APPARATUS SELECTION UNIT LINK ,501 INPUT/ OUTPUT UNIT 507 USER

FIG. 54

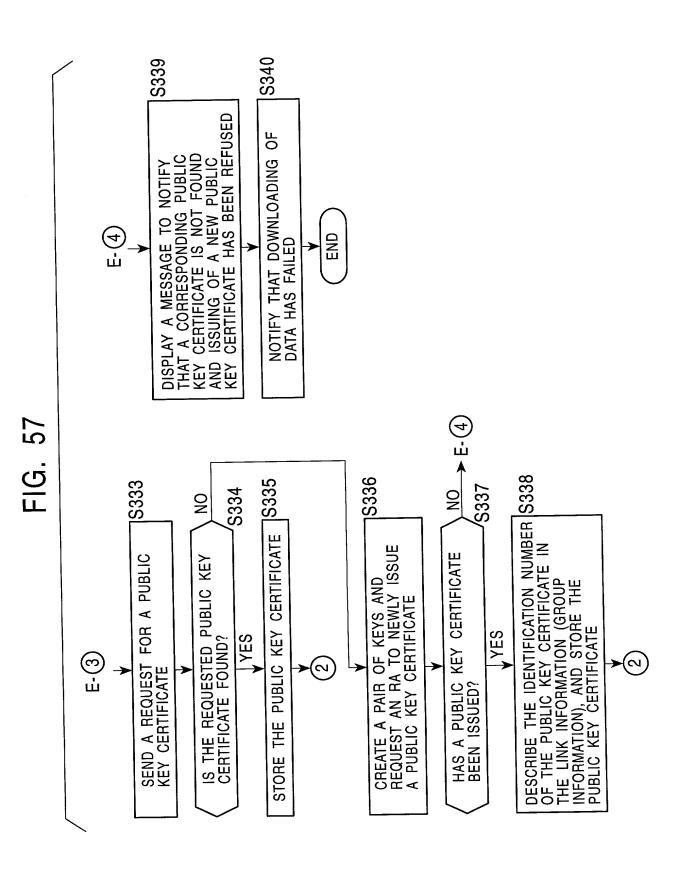




56 / 89



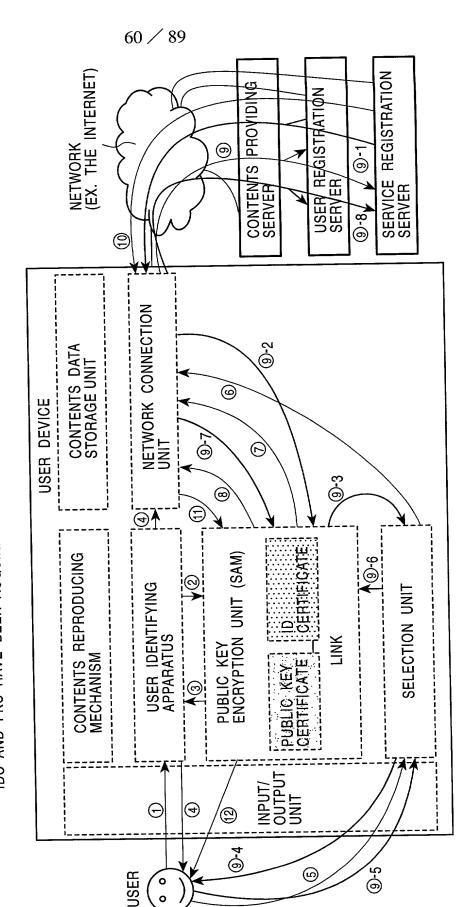
COSTESE DESCRI

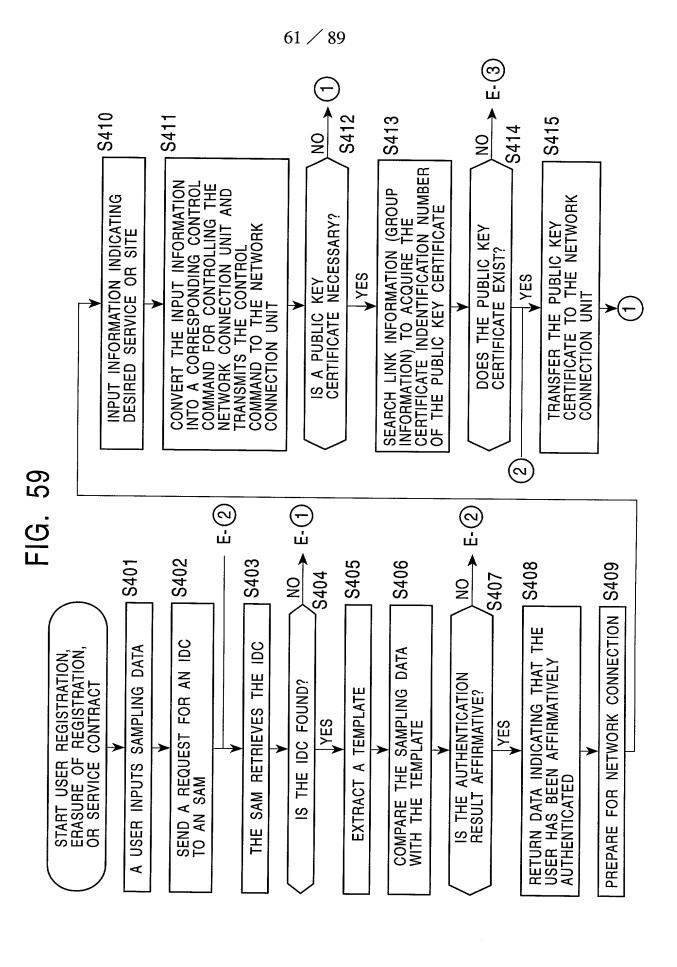


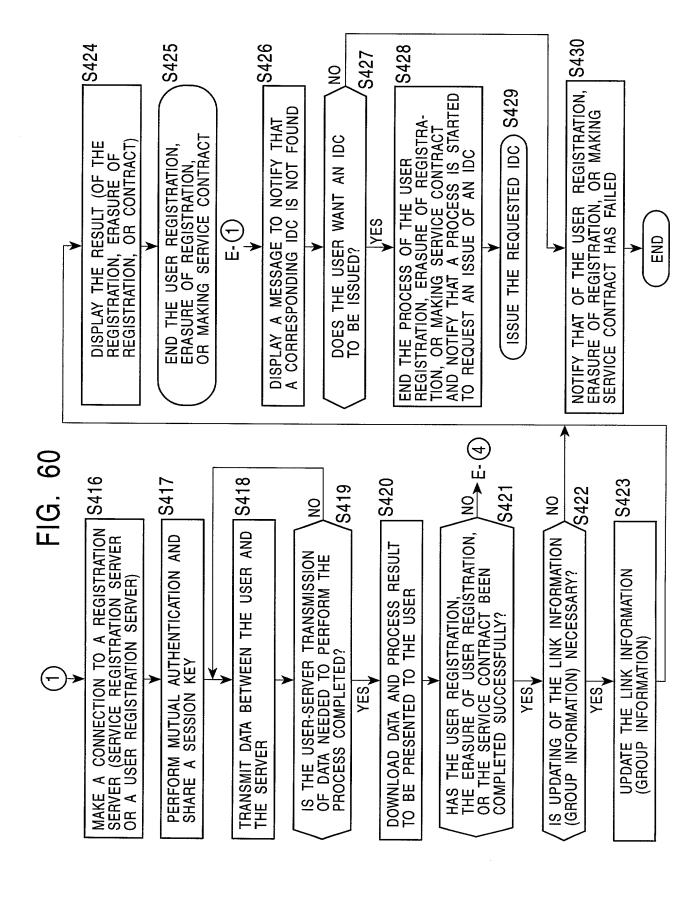
111 | 1880 | 1886 | 1876 | 1876 | 1876 | 1876 | 1876 | 1876 | 1876 | 1876 | 1876 | 1876 | 1876 | 1876 | 1876 |

FIG. 58

PRECONDITION:
•IDC AND PKC HAVE BEEN ACQUIRED







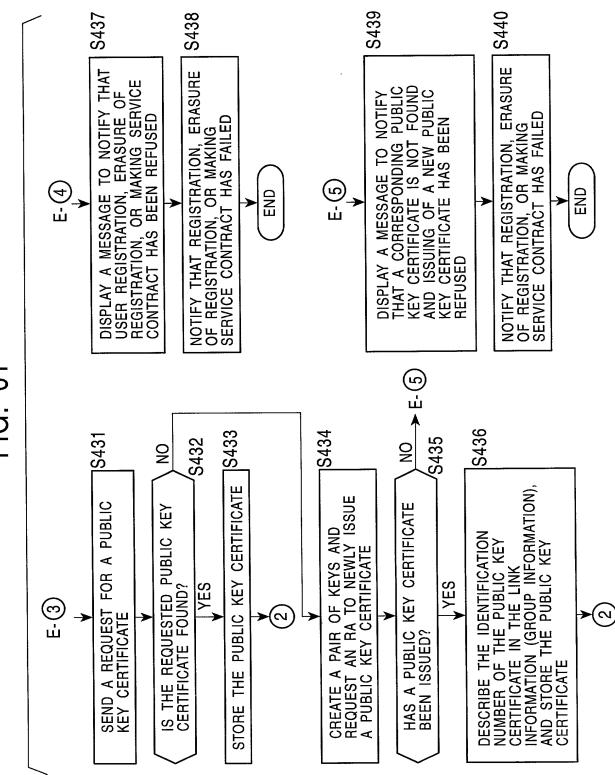


FIG. 61

FIG. 62

PRECONDITIONS:

- . AN IDC OF INTEREST HAS NOT BEEN REGISTERED IN THE USER DEVICE
- THE USER DEVICE HAS NEITHER A PKC NOR A PAIR OF KEYS BUT THE USER DEVICE CAN CREATE THEM
 - AN OFF-LINE PROCEDURE NEEDED TO ISSUE AN IDC HAS BEEN PERFORMED, AND INFORMATION (PIN, TEMPLATE, OR SIGNATURE ENCRYPTED USING A PRIVATE KEY) USED TO CHECK WHETHER A TEMPLATE SUPPLIER IS IDENTICAL TO AN APPLICANT HAS BEEN DETERMINED

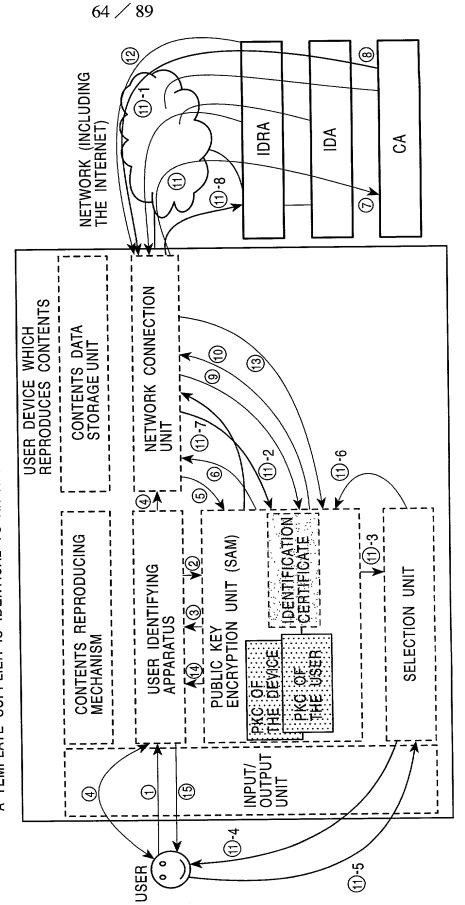
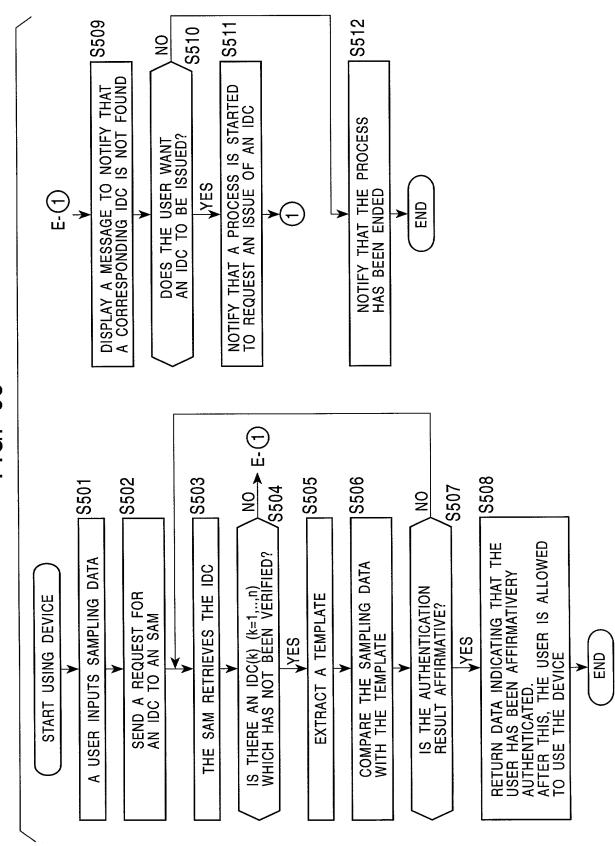
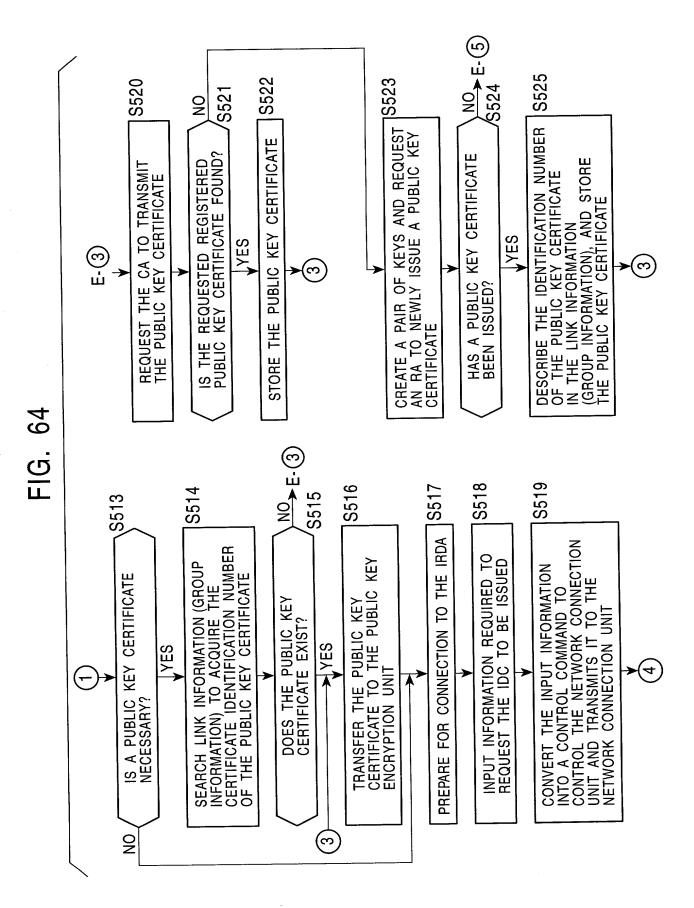


FIG. 63





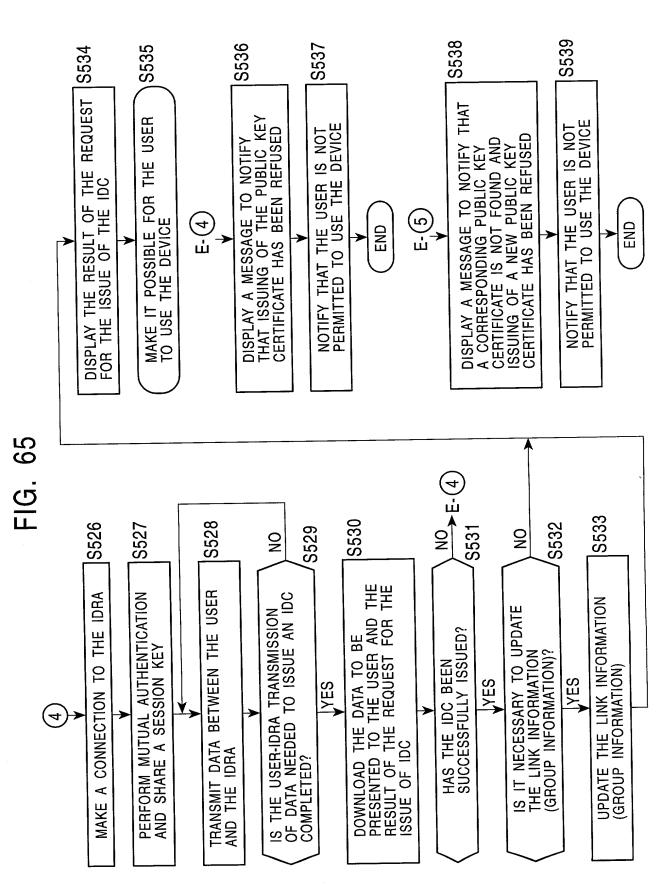
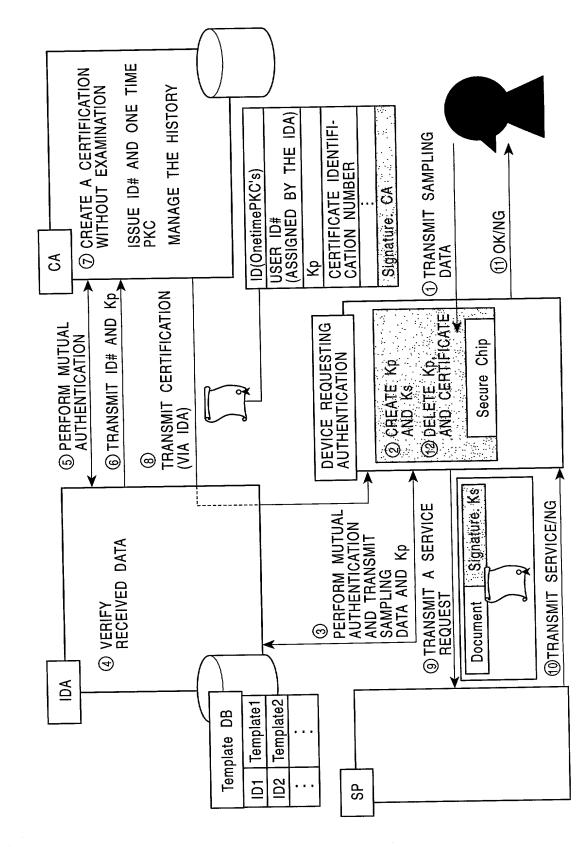


FIG. 66



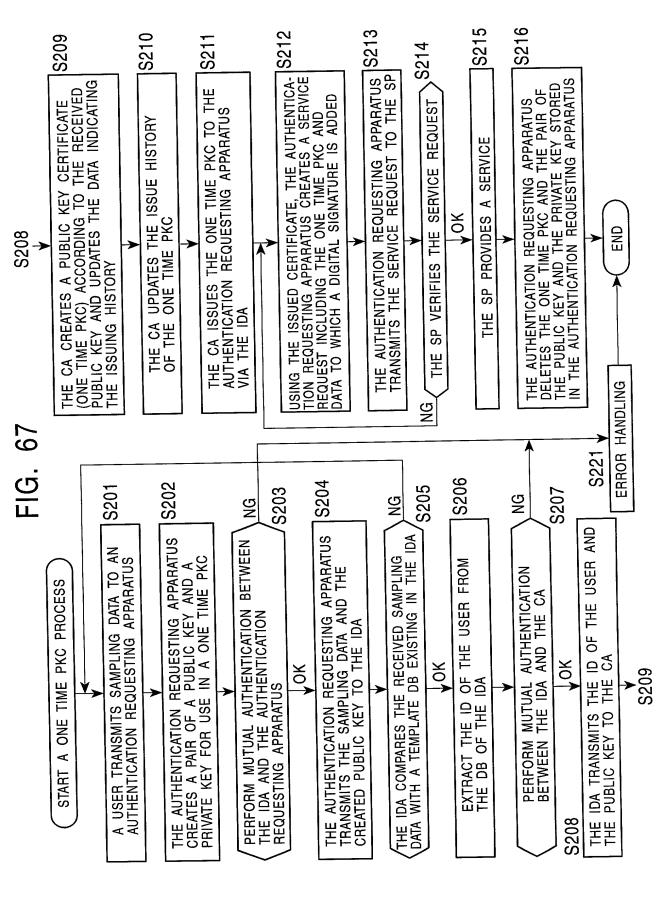
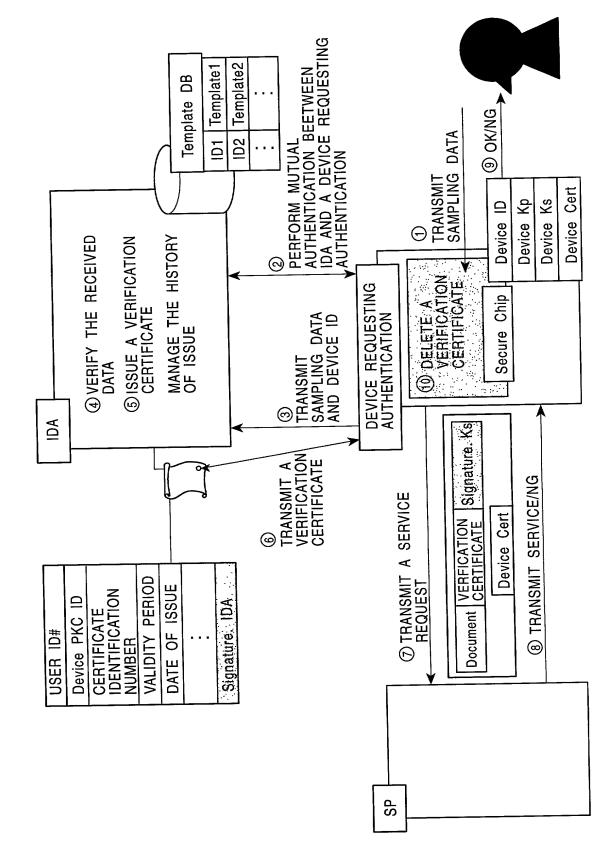
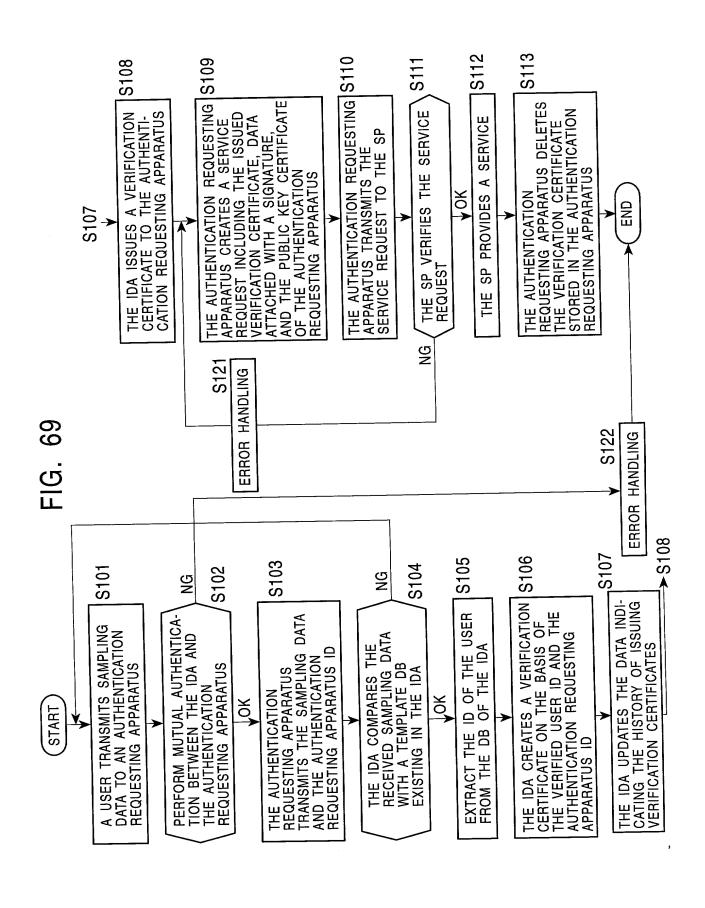


FIG. 68





npr 11.14

ηр

FIG. 70

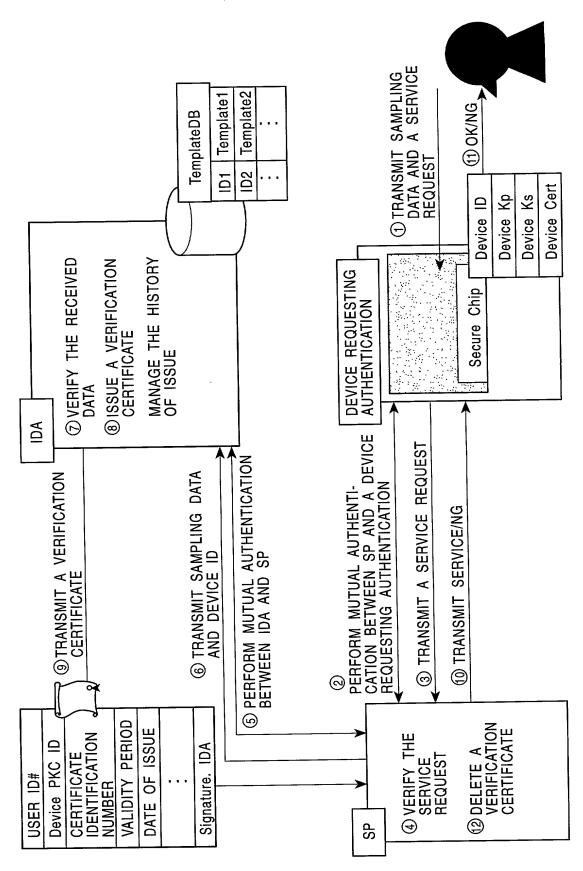


FIG. 71

	Item	Description
Indis- pensable Items	Version	Version
	Serial Number	Identification Number
	signature algorithm Identifier	Signature algorithm
	algorithm parameters	Algorithm Parameters
	Issuer	Identification authority name (in the form of a distinguished name)
	Validity notBefore notAfter	Validty period • Start date • Expiration date
	Subject	Subject Name (in a DN form)
	subject IDA Info subject IDA serial Number subject IDA Unique ID	Information about the identification cartificate of the subject • Certificate number of the identification certificate of the subject • Subject unique ID of the identification cerificate of the subject
	subject PKC info subject PKC serial Number	Information about the public key certificate of the subject Certificate Number of the public key certificate of the subject
	subject PKC Unique ID	Subject unique ID of the public key certificate of the subject
Indispen- sable	IDA Signature	Signature of IDA

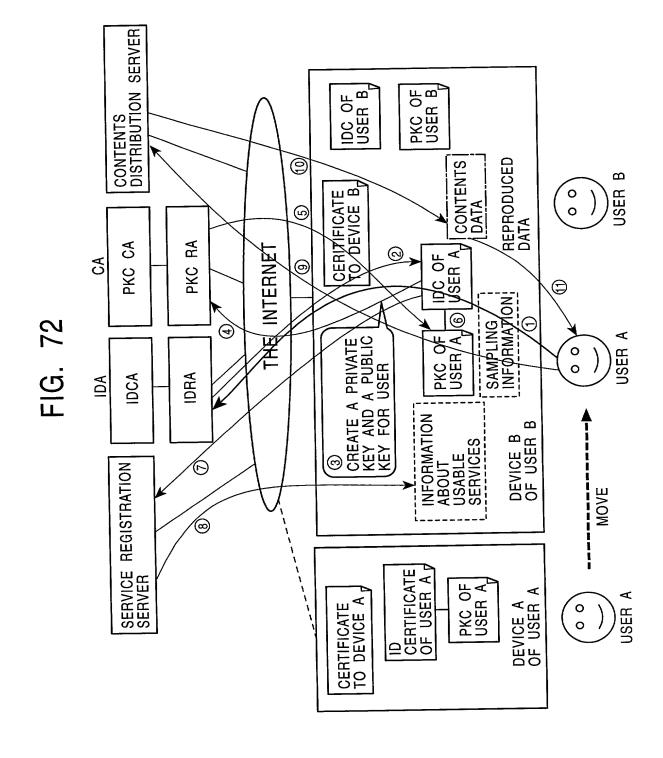


FIG. 73

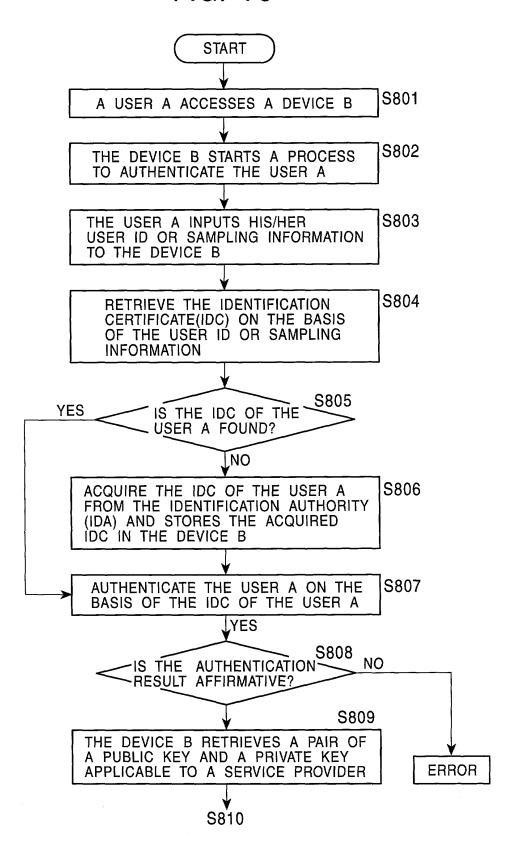


FIG. 74

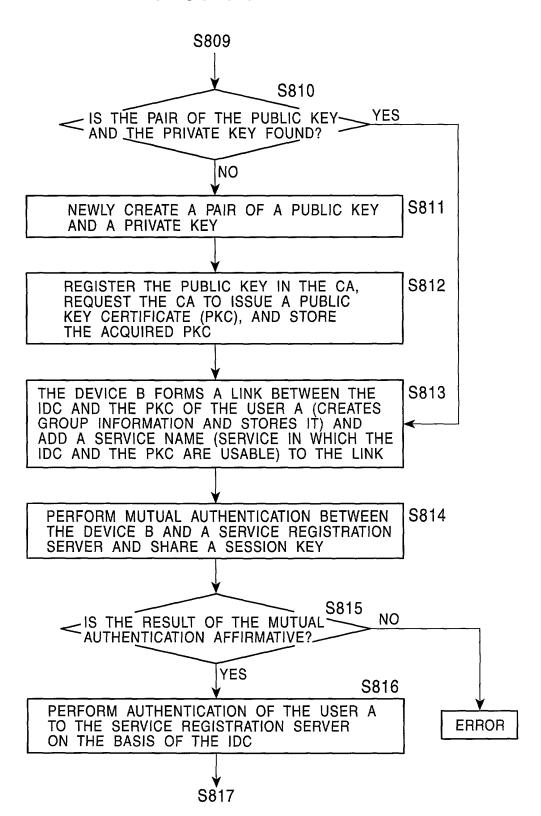
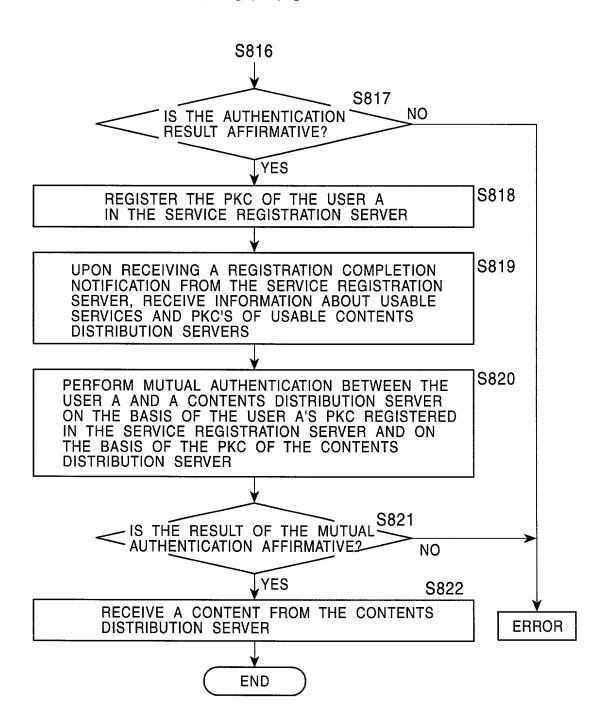


FIG. 75



SERVER

CONTENTS DISTRIBUTION ID CERMIFICATE OF/USER B P REPRODUCED DATA SUCH AS MUSIC OR AN IMAGE CONTENTS 6 USER B 0 CERITIFICATE TO DEVICE B. THE INTERNET, \mathbb{R} CA (9) CA PKC PKC CERTIFICATE OF USER AD \odot USER A (0) 0 SAMPLING 0 DEVICE B OF USER B IDRA IDCA IDA INFORMATION ABOUT USABLE -SERVICES <u>@</u> REGISTRATION MOVE \bigoplus ID CERTIFICATE OF USER A INFORMATION ABOUT USABLE SERVICES SERVICE | SERVER CERTIFICATE TO DEVICE A USER A DEVICE A OF USER A 0

FIG. 77

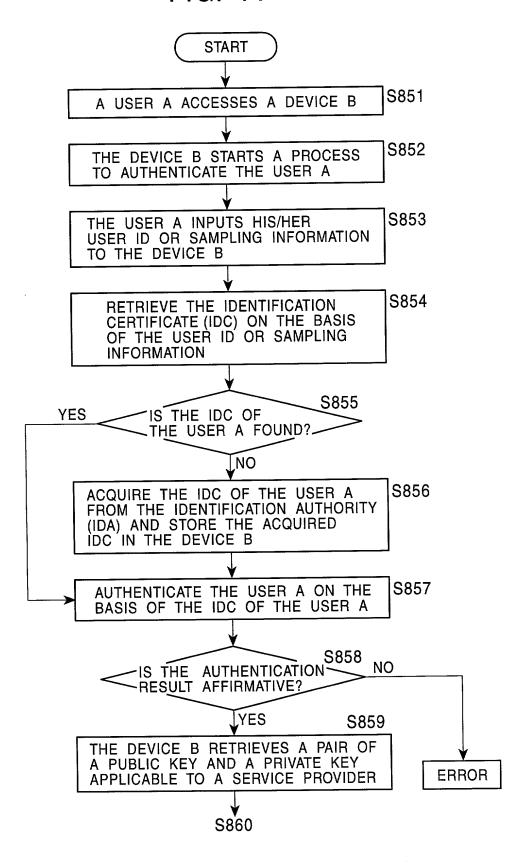


FIG. 78

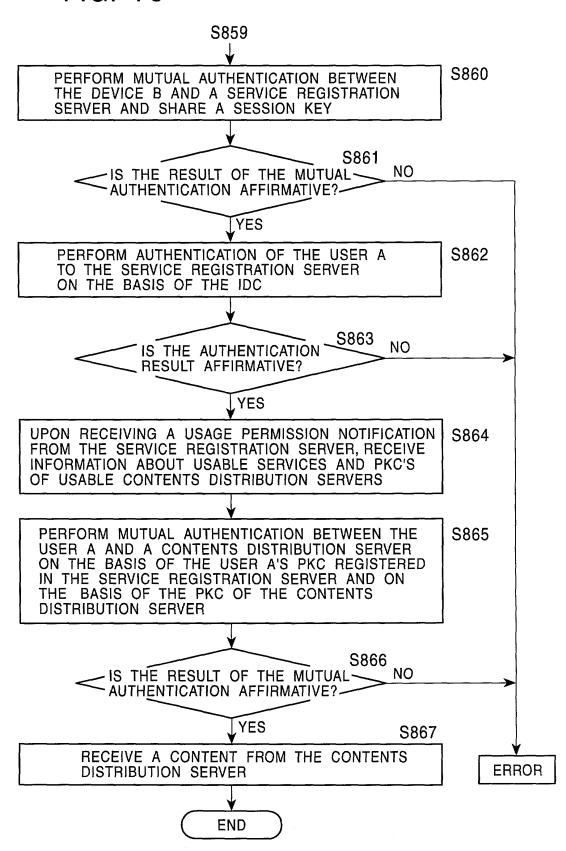
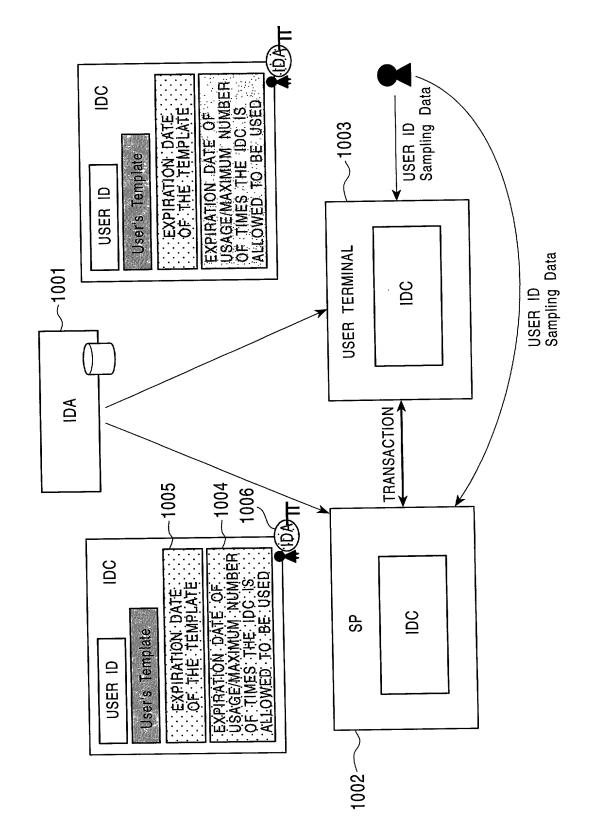


FIG. 79



n n n n n n

· Hal

FIG. 80A

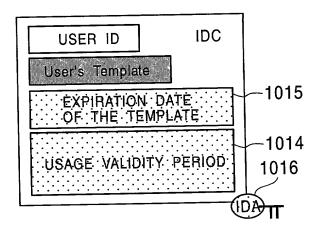


FIG. 80B

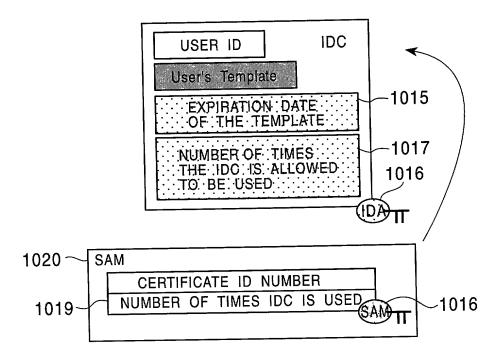


FIG. 81

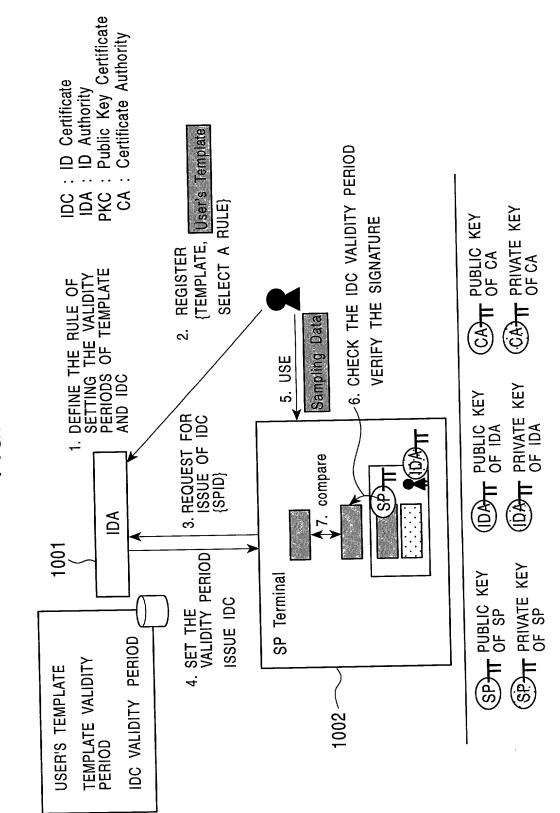
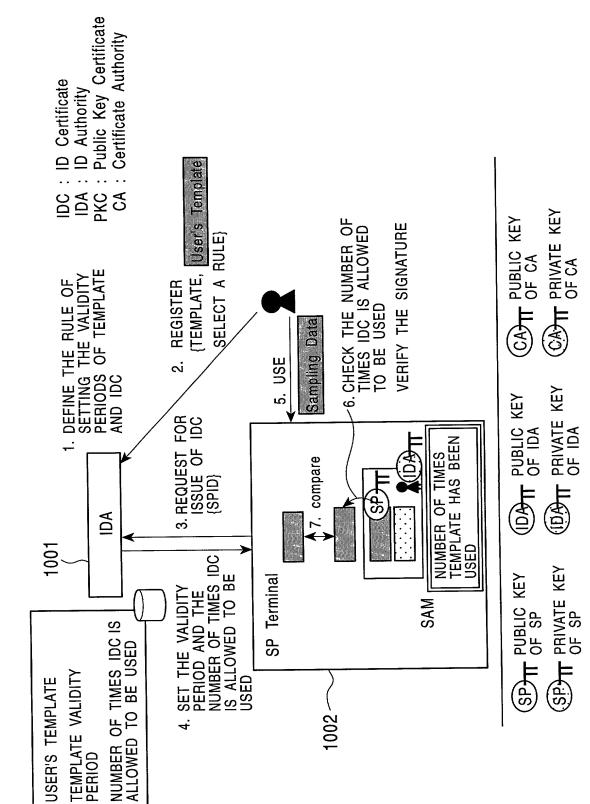


FIG. 82



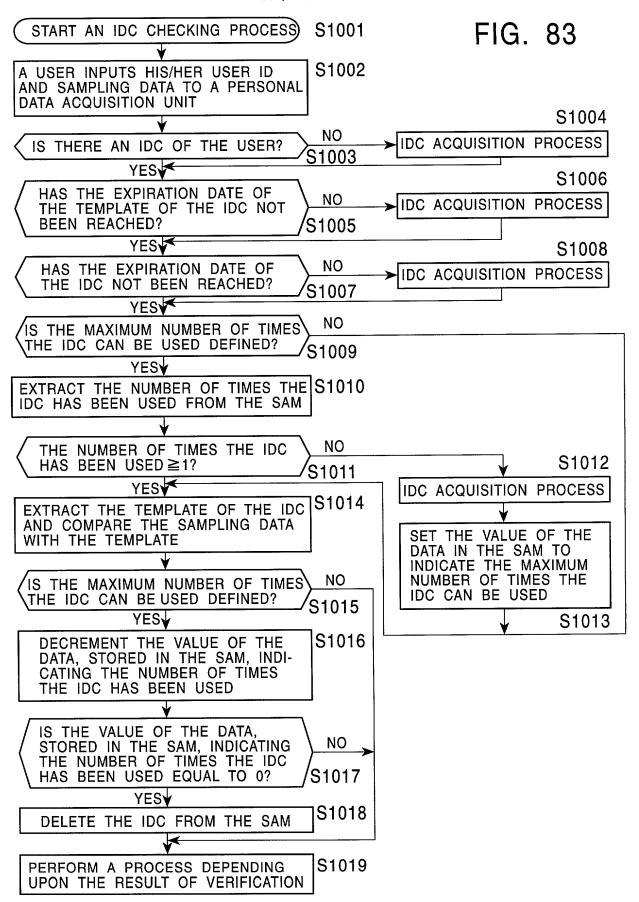


FIG. 84

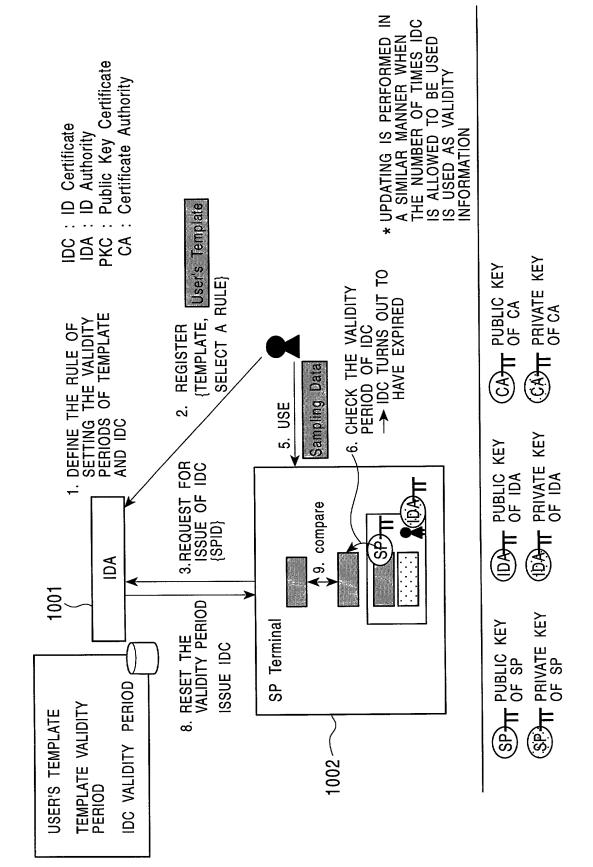


FIG. 85

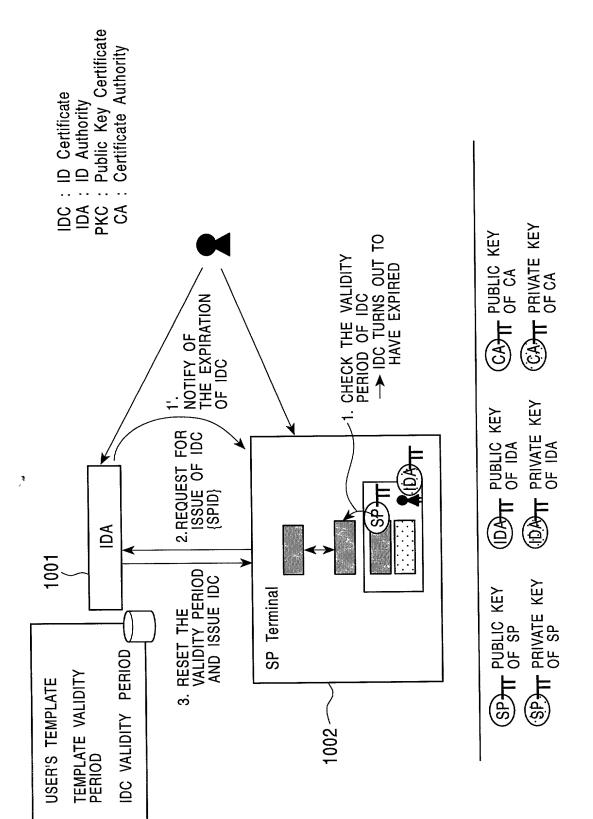


FIG. 86

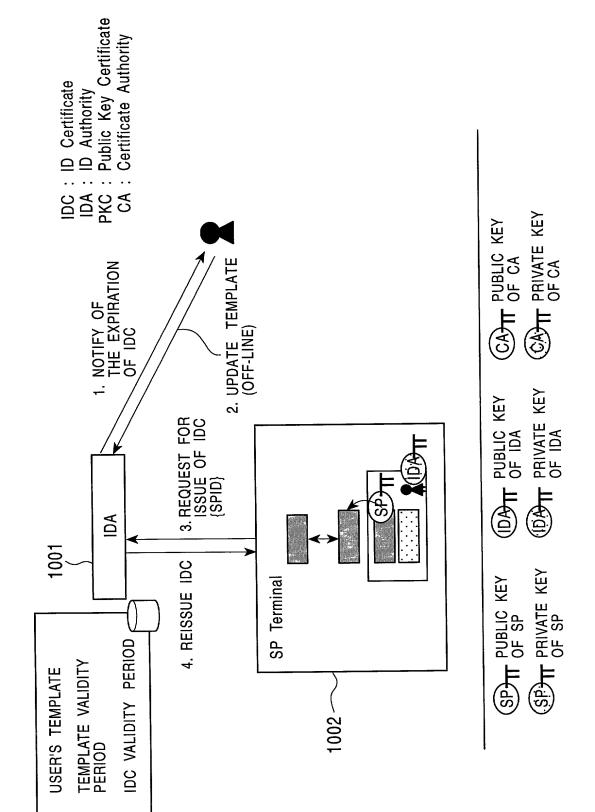


FIG. 87

